PROPUESTA DE SEGURIDAD INFORMÁTICA PARA PROMOVER LA EJECUCIÓN DE TELETRABAJO EN LA MESA DE AYUDA DE UNA EMPRESA DE TELECOMUNICACIONES

ASTRID LILIANA BOHÓRQUEZ SANDOVAL
MAGDA YOHANNA VELÁSQUEZ ARIZA

Trabajo de grado para la obtención del Título de:
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director Trabajo de Grado
Álvaro Escobar Escobar

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE POSGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2015

DEDICATORIA

A mi Padre Celestial que ha movido sus hilos divinos para ubicarme en lugares perfectos y ha puesto junto a mí a personas que con su apoyo me han traído hasta aquí.

Magda Yohanna Velásquez Ariza

A mi madre, hermano, y a Lalo por su apoyo y amor incondicional, en todos los sueños, deseos, proyectos y realizaciones que he emprendido y he logrado.

Astrid Liliana Bohórquez Sandoval

AGRADECIMIENTOS

Damos gracias a Dios, por su inmensa misericordia, por colocarnos en una familia excepcional junto a personas que nos transmiten su amor cada segundo, para quienes un día fuimos un sueño, y que ahora, dedican su vida a cumplir con esmero los nuestros

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE GRÁFICAS

Pág.

INTRODUCCIÓN

El presente trabajo de grado pretende constituirse en un documento de referencia que advierta los beneficios de trascender el enfoque de la concepción del trabajo convencional hacia el Teletrabajo, entendida su realización en condiciones de seguridad, es decir, que observe las características de confidencialidad, integridad y disponibilidad de la información.

Para tal propósito, parte de la formulación de una hipótesis y/o pregunta relacionada con la estrategia de seguridad de la información, que debe estar presente al momento de orientar determinados procesos y actividades hacia el contexto del teletrabajo. Una vez formulado el alcance y objetivos relacionados con la administración del riesgo en la operación del teletrabajo, y los posibles beneficios que se pueden obtener, se realiza una contextualización del marco de referencia desde la dimensión histórica, legal, conceptual y teórica de los conceptos estructurantes del presente trabajo, a saber teletrabajo y seguridad.

Acto seguido, se realiza un abordaje metodológico basado en un tipo de investigación con técnicas descriptivas y explicativas apoyadas en la revisión documental y bibliográfica de los conceptos estructurantes ya mencionados. En específico y como instrumentos de recopilación de información se acude al uso de las entrevistas y a la realización de reuniones en el campo de estudio seleccionado, que para el caso, es la mesa de ayuda de Grandes Clientes de una Empresa de Telecomunicaciones.

Resultado del análisis y estudio de la información obtenida con base en las anteriores técnicas e instrumentos de investigación sobre aquellos procesos que son susceptibles de orientar el manejo de información en teletrabajo en términos confiables, íntegros y disponibles, y la identificación de las necesidades tecnológicas que conlleva dicha tarea, se realiza una propuesta a la mesa de ayuda de Grandes Clientes de una Empresa de Telecomunicaciones sobre la satisfacción de estas necesidades, la definición de los beneficios y aportes.

Finalmente se derivan una serie de conclusiones y recomendaciones sobre el impacto positivo a la implementación en la seguridad de la información del teletrabajo enmarcado en los procesos objeto de estudio, y se plantean posibles procesos igualmente susceptibles de trascender al esquema del teletrabajo en condiciones seguras.

1. JUSTIFICACIÓN

La justificación del presente trabajo derivada del estudio de los procesos y actividades susceptibles en la mesa de ayuda de Grandes Clientes de una Empresa de Telecomunicaciones, como entidad en la cual se realiza el foco de estudio, de orientar el esquema tradicional de realización del trabajo a una modalidad basada en el teletrabajo, obedece a la necesidad, de ratificar el área, procesos, funciones y actividades relacionadas con la mesa de ayuda de la Empresa de Telecomunicaciones previamente identificada como objeto de dicha orientación.

La razón de tal orientación, es la consideración de la naturaleza sensible y critica que administra las peticiones de los usuarios, realiza la gestión y solución de todas las incidencias relacionadas con las tecnologías de la información y comunicación, gestiona la información de los clientes, las soluciones adquiridas, el acceso a las plataformas, el histórico de actividades realizadas, y los informes brindados al cliente final. En definitiva, gestiona todo lo relativo a uno de los principales activos de la Empresa de Telecomunicaciones cuál es la información.

Con base en lo anteriormente mencionado, el problema central que entra a resolver la presente investigación lo constituye la ausencia de una visión integral y estructurada del sistema de gestión de la seguridad de la información, la cual debe preceder la implantación del teletrabajo para el modelo organizacional asociado a la mesa de ayuda de la Empresa de Telecomunicaciones. Dicha labor se ha visto dilatada debido a que no se han formulado requerimientos y lineamientos de seguridad, que garanticen la disponibilidad, integridad y confidencialidad de la información, al igual que la continuidad en la prestación del servicio al cliente que supondría una modalidad basada en el teletrabajo.

Adicionalmente, al examinar los problemas y dificultades de movilidad y sus correspondientes efectos ambientales y de calidad de vida sobre el discurrir y cotidianeidad de una ciudad cosmopolita como Bogotá, y en específico, al revisar la ubicación geográfica del área de mesa de ayuda de la Empresa de Telecomunicaciones, ubicada en la localidad de Usaquén, se advierten descriptores conexos de la problemática en estudio, que igualmente justifican la realización del análisis de la viabilidad de implementación del esquema del teletrabajo para este proceso.

En consecuencia, el presente trabajo procura aportar el estudio y análisis de los beneficios, y ventajas de trasladar los procesos y actividades de los ingenieros de soporte de la mesa de ayuda a una modalidad de teletrabajo suplementario, que observe los elementos esenciales y mínimos de un sistema de gestión seguro de la información. Del mismo modo, pretende constituirse en un documento de referencia que apoye el proceso de toma de decisiones a nivel directivo de la Empresa de Telecomunicaciones en ese sentido, brindando para tal efecto, los elementos conceptuales, explicativos, argumentativos y propositivos sobre dicha implementación.

Debido a las ventajas que produce al implementar la modalidad de teletrabajo para la organización, el área de mesa de ayuda de la Empresa de Telecomunicaciones, tiene la intención de establecer el teletrabajo para los ingenieros de soporte, en los turnos nocturnos inicialmente y ampliarlo a otros horarios, sujeto a los resultados obtenidos con las pruebas preliminares, esta labor se ha visto dilatada debido a que no se han formulado requerimientos y lineamientos de seguridad, que garanticen la disponibilidad, integridad y confidencialidad de la información, al igual que la continuidad en la presentación del servicio al cliente durante la jornada de teletrabajo.

2. PLANTEAMIENTO DEL PROBLEMA

¿Cuál debe ser la estrategia de seguridad de la información que lleve a las directivas de la Empresa de Telecomunicaciones, a implementar la modalidad de teletrabajo sin que se presente afectación de la disponibilidad, integridad y confidencialidad de información vital para el negocio?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Realizar una propuesta de seguridad informática que se constituya en un documento de referencia y apoyo a la decisión del nivel directivo de la Empresa de Telecomunicaciones, al momento de orientar el proceso y procedimientos seleccionados a la modalidad de teletrabajo.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los beneficios y ventajas de orientar la forma tradicional de ejecutar los procesos y actividades en la mesa de ayuda de Grandes Clientes de Empresa de Telecomunicaciones, a la modalidad de Teletrabajo con referencia a los componentes y elementos propios de un sistema de gestión de la seguridad de la información.

- Realizar el levantamiento de información y diagnóstico de los procesos, procedimientos, cargos, y perfiles de la mesa de ayuda de Grandes Clientes de Empresa de Telecomunicaciones que son susceptibles de orientarlos a la modalidad de teletrabajo.

- Elaborar el análisis y estudio de los riesgos probables en seguridad de la información, que pueden estar presentes al momento de orientar el proceso seleccionado al interior de la mesa de ayuda de Grandes Clientes de la Empresa de Telecomunicaciones hacia la modalidad de teletrabajo.

- Proponer controles que permitan administrar los riesgos en condiciones estándares de disponibilidad, integridad y confidencialidad de la información, presentes en el proceso seleccionado de la mesa de ayuda de Grandes Clientes de la Empresa de Telecomunicaciones a implementar en la modalidad de teletrabajo.

4. MARCO TEÓRICO

4.1 BREVE RETROSPECTIVA HISTÓRICO DEL TELETRABAJO

Con la aparición de la internet en la década de los 60´s, se cimenta unos de los pilares fundamentales, que en definitiva se ha constituido en un elemento estructural de las soluciones de desarrollo tecnológico y telecomunicaciones de la información, el cual ha venido aumentando su uso exponencial a lo largo de todos estos años.

En la década de los 70's en los EE.UU, se incorpora el estudio al término de "telecommuting", concepto ideado por el físico Jack Nilles para solucionar el problema de la falta de combustible y de la alta contaminación. Dicho estudio se encontraba basado en la idea de "llevar el trabajo al trabajador y no el trabajador al trabajo"[1]. Si bien es cierto, con el desarrollo de esta conceptualización se advierten los primeros esfuerzos orientados a cambiar el paradigma de realización del trabajo, también lo es que para la época las telecomunicaciones, como pilares fundamentales del mismo, no se encontraban adecuadas para dinamizar el concepto que la postre se convertiría en Teletrabajo.

Las posteriores décadas, se caracterizan por un desarrollo fuerte en materia de telecomunicaciones, desarrollo que incorpora nuevos elementos adicionales de base hacia la estructuración del teletrabajo como una alternativa innovadores de acometer las actividades de las organizaciones.

Como alternativa, el teletrabajo se constituye en una opción tecnológica que ha brindado soluciones a necesidades específicas que presenta el contexto global laboral moderno en las organizaciones. Es de señalar, que como primeros indicios concretos se realizan pruebas piloto y se da inicio formal con esta alternativa, ejercicios que se desarrollan en California, San Francisco. Adicionalmente es de mencionar que la condición geográfica de este estado caracterizada por frecuentes desastres naturales, conllevó y se constituyó en un factor determinante para decidirse por la modalidad de teletrabajo, como alternativa de solución identificada por los ciudadanos norteamericanos de esta región para los momentos de crisis que generan los eventos naturales mencionados.

[1]Bogotá es una Ciudad para el Teletrabajo: Jack Nilles. Disponible: http://www.colombiadigital.net/teletrabajo/item/3542-bogot%C3%A1-es-una-ciudad-para-el-teletrabajo-c.html

Como otro antecedente histórico del teletrabajo en otro contexto geográfico como es la Unión Europea, se advierte que como resultado de negociaciones sostenidas entre los interlocutores sociales europeos, se ratifica el acuerdo marco europeo sobre el teletrabajo el 16 de julio de 2002. Este acuerdo permitió la masificación del teletrabajo en todos los Estados miembros de la Unión Europea.

Ahora bien, al examinar el contexto de América Latina, se advierte en el documento "Lista de indicadores para el eLAC2015" tomado de los archivos de la CEPAL los siguientes párrafos introductorios, a saber:[2]

"En noviembre de 2010 se aprobó el Plan de acción sobre la sociedad de la información y el conocimiento de América Latina y el Caribe (eLAC2015), durante la III Conferencia ministerial sobre la sociedad de la información en América Latina y el Caribe, realizada en Lima, Perú. El plan, que plantea que las tecnologías de la información y de las comunicaciones (TIC) son instrumentos de desarrollo económico y de inclusión social, es una estrategia de largo plazo con miras hacia el 2015, acorde con los Objetivos de Desarrollo del Milenio (ODM) y la Cumbre Mundial de la Sociedad de la Información (CMSI).

El mecanismo de seguimiento de eLAC2015 está conformado por la conferencia ministerial de seguimiento, la mesa de coordinación y los puntos focales de los países miembros, además de observadores en representación de la sociedad civil, el sector privado y la comunidad técnica de Internet de la región. El plan reconoce catorce grupos de trabajo en las áreas de acceso e infraestructura, gobierno electrónico e interoperabilidad, desechos tecnológicos, TIC y salud, innovación y apropiación de TIC en la MPYME, contenidos digitales, software y servicios de tecnología de la información, teletrabajo, marco normativo de la sociedad de la información, comercio electrónico, gobernanza de Internet, género, financiamiento y desarrollo digital para la educación."

Al observar el anterior párrafo se evidencia que el teletrabajo se constituye en un grupo de trabajo objeto de intervención Plan de acción sobre la sociedad de la información y el conocimiento de América Latina y el Caribe (eLAC2015); es decir, existe un esfuerzo de los países miembros en el tema específico del teletrabajo.

[2] CEPAL. Lista de indicadores para el eLAC2015. Disponible: http://archivo.cepal.org/pdfs/2013/S2013089.pdf

Como otra referencia pero ya al nivel de países del sur de América, se encuentra la legislación implementada en Argentina con la Ley 3498 de 2010 "Régimen jurídico del Teletrabajo en relación de dependencia", Brasil con la Ley 5405 de 2008 "Se reglamenta el teletrabajo a distancia conceptúa y disciplina las relaciones de teletrabajadores (…)", Chile Proyecto de ley que impulsa el trabajo a distancia, y Colombia mediante la regulación que se dio con la Ley 1221 de 2008 mediante la cual "Se promueve el teletrabajo y la generación de autoempleo".

4.2 TELETRABAJO EN COLOMBIA

La referencia del teletrabajo en Colombia como modalidad alternativa de ejecutar el trabajo y nueva forma laboral, encuentra soporte legal con la expedición de la Ley 1221 de 2008, la cual define el mismo como: "Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación - TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo". (Artículo 2, Ley 1221 de 2008)[3]

Como modalidades, tipos y características del teletrabajo o tipos de teletrabajador en Colombia, la Ley prevé, bajo el supuesto de que los trabajadores obtengan diferentes alternativas para ejecutar su trabajo, y ejercer control sobre su tiempo, tareas, objetivos, calidad de vida y aumento de productividad para la organización.

4.2.1 Modalidades. A continuación se expresan las modalidades definidas en (Artículo 2, Ley 1221 de 2008)

4.2.1.2 Teletrabajo Autónomo: Trabajadores independientes o empleados que se valen de las TIC para el desarrollo de sus tareas, ejecutándolas desde cualquier lugar elegido por él.

[3] CONGRESO DE LA REPUBLICA. Ley 1221 de 2008. Disponible: http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-571.html

4.2.1.3 Teletrabajo Suplementario: Trabajadores con contrato laboral que alternan sus tareas en distintos días de la semana entre la empresa y un lugar fuera de ella usando las TIC para dar cumplimiento. Se entiende que teletrabajan al menos dos días a la semana.

4.2.1.4 Teletrabajo Móvil: Trabajadores que utilizan dispositivos móviles para ejecutar sus tareas. Su actividad laboral les permite ausentarse con frecuencia de la oficina. No tienen un lugar definido para ejecutar sus tareas. (Artículo 2, Ley 1221 de 2008)[4]

4.2.2 Características del Teletrabajo. Las características del Teletrabajo son interpretadas como:

- Una actividad laboral que se lleva a cabo fuera de la organización en la cual se encuentran centralizados todos los procesos.
- La utilización de tecnologías para facilitar la comunicación entre las partes sin necesidad de estar en un lugar físico determinado para cumplir sus funciones.
- Un modelo organizacional diferente al tradicional que replantea las formas de comunicación interna de la organización y en consecuencia genera nuevos mecanismos de control y seguimiento a las tareas.[5]

En las modalidades anteriormente mencionadas, definidas por la ley colombiana, y dada la propuesta del teletrabajo en la empresa de Telecomunicaciones, se iniciará con una prueba piloto donde se adoptará la modalidad del teletrabajo, usando las TIC en un lugar distinto a la empresa, con el seguimiento y control de gestión de los trabajadores, sugiriendo dos días a la semana definidos por la empresa.

Al revisarse el concepto de teletrabajo y para efectos de cumplir con el objetivo del trabajo, es indispensable conocer su definición, teorías, modalidades, características, legislaturas, y todo lo que se debe tener en cuenta para su implementación conforme a un análisis de seguridad en la información.

[4] LIBRO BLANCO DEL ABC DEL TELETRABAJO EN COLOMBIA VERSION 3.0 Ministerio de las Tecnologías de la Información y las Comunicaciones, Bogotá D.C Colombia Digital.

[5] LIBRO BLANCO DEL ABC DEL TELETRABAJO EN COLOMBIA VERSION 3.0 Ministerio de las Tecnologías de la Información y las Comunicaciones, Bogotá D.C Colombia Digital

4.3 ELEMENTOS DE DESARROLLO DEL TELETRABAJO EN COLOMBIA

En Colombia. Se establece un reconocimiento y garantías laborales a los Teletrabajadores, con la ley 1221 de 2008. Tiene como objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).[6] Para asegurar la igualdad laboral de los teletrabajadores a los trabajadores del sector privado y público, se crearon aspectos laborales especiales e impulsar la cultura del teletrabajo en el país, se crea el decreto 884 de 2012.[7]

A partir del año 2012, en Colombia se ha promovido e impulsado la cultura del Teletrabajo, con participación del Ministerio de Tecnologías de información y las Comunicaciones en unión con la Corporación Colombia Digital y el Ministerio de Trabajo. En el mes de julio de 2012, se realizó la primera feria internacional del Teletrabajo, para brindar información sobre los beneficios e impactos de la modalidad laboral a distancia, el evento fue asistido por el gobierno, expertos nacionales internacionales, empresarios y sociedad en general.[8] Cabe mencionar que las entidades del estado anteriormente mencionadas, adoptó asesorías para esta práctica laboral. A partir de ese momento, empresas públicas y privadas han participado y optado por esta nueva modalidad.[9]

Adicionalmente, el gobierno nacional, los Ministerios TIC y del Trabajo, desarrollaron una guía metodológica completa, llamada “El Libro Blanco ABC del teletrabajo en Colombia”, para aquellas empresas del país interesadas en implementar un modelo de teletrabajo, como alternativa para aumentar su productividad y mejorar la calidad de vida de los empleados. El lanzamiento del Libro Blanco fue en la ciudad de Medellín, en noviembre de 2012. Luego fue lanzada una segunda versión de esta guía en marzo del 2014, realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio del Trabajo y la Corporación Colombia Digital, agregando dos capítulos orientados a temas jurídicos y de implementación tecnológica. [10] Posteriormente

---

[6] Decreto reglamentario. Ley 1221 de 2008 teletrabajo. Colombia, 2008. Disponible: http://mintrabajo.gov.co/component/.../doc.../1876-ley1221de2008.html

[7] Decreto 884 de 2012. Ministerio de trabajo. Disponible: http://www.mintic.gov.co/portal/604/articles-3638_documento.pdf

[8] A Colombia llega la Feria Internacional del Teletrabajo. Disponible en el sitio web: http://www.mintrabajo.gov.co/julio-2012/711-a-colombia-llega-la-feria-internacional-del-teletrabajo.html

[9] Colombia Digital. Una nueva firma del pacto por el teletrabajo. Disponible: http://colombiadigital.net/actualidad/noticias/item/7434-una-nueva-firma-del-pacto-por-el-teletrabajo.html

[10] Colombia Digital. Disponible: http://www.colombiadigital.net/actualidad/noticias/item/6589-descargue-la-segunda-entrega-del-libro-blanco-del-teletrabajo-en-colombia.html

los contenidos fueron actualizados, recomendaciones jurídicas y orientación sobre el uso de formatos para cada procedimiento; actualmente se tiene la versión 3.0 del Libro Blanco ABC del teletrabajo en Colombia.

4.4 BENEFICIOS Y DESVENTAJAS

Los Beneficios que se tienen para la implementación del teletrabajo en las organizaciones, se presentan no solo para la organización sino también para los trabajadores. Se referencia el Libro Blanco ABC del Teletrabajo en Colombia**.**[11]

4.4.1 Beneficios para la organización. Los beneficios que se tienen establecidos en la organización, se mencionan a continuación:

- Mayor productividad
- Reducción de costos físicos
- Reducción del ausentismo y retiro voluntario de empleados
- Control y seguimiento en las tareas programadas a los trabajadores, a través de herramientas tecnológicas
- Mayor índice de retención del personal capacitado
- Preferencia de un empleo con trabajo móvil
- Aporte al mejoramiento de la movilidad en la ciudad
- Contribución a la calidad de vida de los trabajadores y su desarrollo

4.4.2 Beneficios para los trabajadores. Para los trabajadores se encuentran definidos como:

- Reducción de tiempo por desplazamientos
- Reducción de costos obtenidos por desplazamientos
- Mejora en la salud, al consumir alimentos preparados en el hogar y al disminuir el estrés, producido por los desplazamientos y gastos asociados
- Impacto ambiental producido en cada uno de los trabajadores, de acuerdo al consumo de energía y reducción en desplazamientos
- Mejora su relación con familiares y amigos

[11] LIBRO BLANCO EL ABC DEL TELETRABAJO EN COLOMBIA VERSION 1.0. Ministerio de las Tecnologías de la Información y las Comunicaciones, Bogotá D.C Colombia Digital.

4.4.3 Desventajas del teletrabajo. El modelo de teletrabajo, indudablemente requiere el uso de las tecnologías de información, un computador y conexión inalámbrica a Internet, son elementos esenciales para realizar el teletrabajo. Pero al utilizar esta clase de tecnología, se presentan problemas y riesgos a los que se deben tener en cuenta.

Para esta situación, se deberá definir un sistema de gestión de seguridad de la información, identificar los riesgos a los que podría estar expuesto, con sus adecuadas medidas de prevención y corrección. Y desde luego, optar estrategias de concientización**.**

4.5 MARCO LEGAL

En Colombia inicia propuestas de legislaciones sobre el Teletrabajo, en julio de 2008. El Congreso de la República de Colombia expidió la Ley 1221, definiendo el teletrabajo como "una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros mediante soportes TIC, para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo"[12] y otras relacionadas a las Tecnologías de la Información y la Comunicación.

4.5.1 Ley 1221 del 2008: Establece el reconocimiento del teletrabajo en Colombia como modalidad laboral, promueve y regula el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones. Regula el Teletrabajo suplementario, autónomo y móvil; garantizando los mismos derechos de un trabajador formal. Así mismo, formula política pública de fomento al Teletrabajo.

4.5.2 Sentencia C-337 del 2011: Protección integral en materia de Seguridad Social del teletrabajador, garantizando distintos beneficios como el subsidio familiar.

---

[12] Decreto reglamentario. Ley 1221 de 2008 teletrabajo. Colombia, 2008. Disponible: http://mintrabajo.gov.co/component/.../doc.../1876-ley1221de2008.html

4.5.3 Decreto 0884 del 2012: Reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones. Establece las condiciones de contrato referente a la vinculación de teletrabajo a través de medios tecnológicos. Además establece medidas de seguridad informática, riesgos profesionales y obligaciones de las ARL. Igualmente establece condiciones laborales especiales del teletrabajo que deben cumplir las entidades del sector público y privada.

4.5.4 Resolución 3559 del 2013: Se estableció el día 4 de septiembre de 2013, el plan de acción para implementar el teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones.

4.5.5 Resolución 4950 del 2013: Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se amplía la vigencia el día 13 de diciembre de 2013, los cargos teletrabajables establecidos en la Resolución 3559 para la prueba piloto de teletrabajo y se dictan otras disposiciones.

4.5.6 Ley 527 de 1999: Reglamenta y define el acceso y uso de los mensajes de datos, del comercio electrónico, firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

4.5.7 Ley 1266 del 2008: Se dictan disposiciones generales del Hábeas Data, la cual regula el uso de la información sobre datos personales, financieros, crediticia, comercial

4.5.8 Ley 1273 de 2009: Ley que reglamenta y crea un nuevo bien jurídico tutelado, denominado “De la protección de la información y de los datos”, modificando el Código penal Colombiano.

4.5.9 Ley 1341 de 2009: Define los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.

4.5.10 Ley 1581 del 2012: Se dictan disposiciones generales para la Protección de Datos Personales, con el objetivo de desarrollar el derecho constitucional que tienen todas las personas de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de

la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. [5]

4.5.11 Decreto 2364 de 2012: Reglamenta el artículo 7 de la ley 527 de 1999, sobre la firma electrónica y firmas digitales y se dictan otras disposiciones.

4.5.12 Decreto 1377 del 2013: Reglamenta la Ley 1581 del 2012. con aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas.[13]

4.6 MARCO CONCEPTUAL

4.6.1 Sistema de Información: Es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento de una empresa para conseguir sus objetivos.

4.6.2 Definiciones: Se mencionan a continuación algunas definiciones en cuanto al sistema de información:

Según Whitten, Bentley y Dittman un sistema de información "es un conjunto de personas, datos, procesos y tecnologías de la información que interactúan para recoger, procesar, almacenar y proveer la información necesaria para el correcto funcionamiento de la organización."[14]

Andreu, Ricart y Valor definen a los sistemas de información "como el conjunto formal de procesos que opera con un conjunto estructurado de datos de acuerdo a las necesidades que una organización, recopila, elabora y distribuye la información necesaria para la operación de dicha organización y para las actividades de dirección de control correspondientes, apoyando al menos en parte, la toma de

[13] Decreto 1377 Consulta de la norma. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

[14] Jeffrey L. Whitten, Lonnie D. Bentley, Kevin C. Dittman . Systems Analysis and Design Methods. McGraw-Hill Irwin, 2004

decisiones necesaria para desempeñar las funciones y procesos de negocio de acuerdo con su estrategia" .[15]

Teniendo en cuenta dichas definiciones los sistemas de información son una ficha importante en el crecimiento y sostenimiento de la empresa misma y todo el manejo, procesamiento, o cualquier interacción con la información debe estar alineado con los objetivos de negocio que la organización maneja.

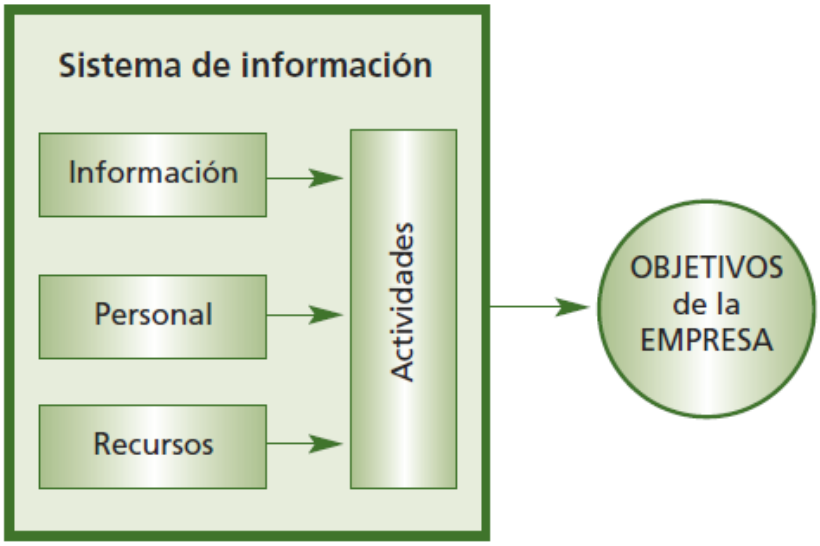
En las organizaciones se emplean gran cantidad de datos como son: datos de los productos, datos de clientes, datos de empleados, datos de la entrega de producto, entre otros; dichos datos juegan un papel significativo en las organizaciones y deben ser almacenados, gestionados, y procesados, y es allí en donde los sistemas de información entran como parte importante del pleno desarrollo de la organización.

4.6.3 Elementos de un Sistema de Información: En un sistema de información, se encuentran unos elementos básicos que interactúan entre sí, para lograr un objetivo común dentro de la organización, a continuación se muestra en la Figura 1, dichos elementos[16]:

[15] ANDREU, R., RICART, J. E. y VALOR, J. (1996): Estrategia y Sistemas de Información, 2ª Edición, McGraw-Hill, pag. 13.

[16] Purificación Aguilera. Seguridad Informática, 2010 Editex

Figura 1. Elementos de un sistema de información



Fuente: Editex - Seguridad informática

- Recursos. Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.
- Equipo humano. Compuesto por las personas que trabajan para la organización.
- Información. Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.
- Actividades que se realizan en la organización, relacionadas o no con la informática.

4.6.4 Objetivos de un Sistema de Información: Algunos de los principales objetivos de los sistemas de información, son:

- Proporcionar datos oportunos y exactos que permitan tomas decisiones acertadas y mejorar la relación entre los recursos de la empresa.
- Garantizar información exacta y confiable, así como su almacenamiento de tal forma que esté disponible cuando se necesite.

- Servir como herramienta para que los gerentes realicen planeación, control y toma de decisiones en sus empresas.[17]

4.6.5 La importancia de Proteger la información: La información es un activo significativo, en la sociedad actual cuanta más información se tiene a disposición, mayores posibilidades se tienen de adaptarse y sobresalir en mundo que le rodea. La información es a menudo uno de los activos más importantes que una empresa posee ya que la misma marca la diferencia y proporciona ventajas que llevan a dicha empresa u organización a ser más exitosa.

La información se puede clasificar en diferentes categorías con el fin de controlar el acceso a la misma en función de su importancia, su sensibilidad y su vulnerabilidad al robo o al mal uso, basado en esta clasificación las organizaciones deciden asignar más recursos para controlar la información que tiene mayor sensibilidad.

Las organizaciones clasifican la información de diferentes maneras con el fin de gestionar de forma diferente aspectos de su manejo, la información destinada a uso interno que se entiende generalmente puede ser vista por los empleados, contratistas y proveedores de servicios, pero no por el público en general. Este tipo de información suele ser menos restringida, ya que no se gasta mucho tiempo y dinero en la protección, debido a que no supera el valor de la información o el riesgo de su divulgación.

Las empresas pueden tener información confidencial, como los planes de investigación y desarrollo, los procesos de fabricación, la información corporativa estratégica, las descripciones de procesos, las listas de clientes y la información de contactos, las proyecciones financieras e informes de ganancias, que son para uso interno exclusivo; la pérdida o robo de información de este tipo podría violar la privacidad de las personas, reducir la ventaja competitiva de la empresa, o causar daños a la empresa.

La información secreta puede incluir secretos comerciales, como fórmulas, detalles de producción, y otra propiedad intelectual, metodologías y prácticas que describen cómo se prestan los servicios de propiedad, los planes de investigación,

[17] UNIVERSIDA DEL CAUCA. Conceptos Básicos de Sistemas de Información [En Línea] <http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm> [citado en 5 Noviembre de 2014]

códigos electrónicos, contraseñas y claves de cifrado. Si se da a conocer, este tipo de información puede dañar gravemente la ventaja competitiva de la empresa. El acceso por lo general se limita a sólo unas pocas personas o departamentos dentro de una empresa y rara vez se da a conocer fuera de la empresa.

En algunos sectores de actividad, la protección de la información en la organización no es sólo deseable, es obligatoria. [18]

4.7 SEGURIDAD DE LA INFORMACIÓN.

Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientadas a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.[19]

El Comité de Sistemas de Seguridad Nacional (CNSS) define seguridad de la información como la protección de la información y sus elementos críticos, incluidos los sistemas y hardware que utilizan, almacenar y transmitir que información.

El propósito de seguridad de la información es proteger los recursos valiosos de la organización, como la información, hardware y software; a través de la selección y aplicación de las salvaguardias adecuadas, la seguridad ayuda a la misión de la organización mediante la protección de sus recursos físicos y financieros, la reputación, la posición legal, empleados y otros activos tangibles e intangibles.

El valor de la información proviene de las características que posee. Cuando una característica de información cambia, el valor de esa información aumenta, normalmente disminuye.

[18] Mark Rhodes – Ousley , Information Security segunda edición, Mac Graw Hill 2013

[19] Purificación Aguilera. Seguridad Informática, 2010 Editex

4.7.1 Principios de la Seguridad Informática: Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

NIST standard FIPS 199 (Normas para la Seguridad Categorización de Información Federal y Sistemas de Información) lista confidencialidad, integridad y disponibilidad como los tres objetivos de seguridad de la información y de los sistemas de información. En la Figura 2, se visualiza los objetivos de seguridad de la información.

Figura 2. Objetivos de seguridad de la información

Fuente: http://www.ceisufro.cl/fileadmin/user_upload/triangulo.jpg

FIPS PUB 199 ofrece una caracterización útil de estos tres objetivos en términos de requisitos y la definición de una pérdida de seguridad en cada categoría:

• Confidencialidad: La preservación de las restricciones autorizadas sobre el acceso y la divulgación de la información, incluidos los medios para la protección de la intimidad personal y propiedad de la información. Una pérdida de confidencialidad es la divulgación no autorizada de información.

La confidencialidad se refiere a la restricción del acceso a los datos sólo a aquellos que están autorizados para utilizarlo. En términos generales, esto significa un único conjunto de datos se puede acceder a una o más personas o sistemas autorizados, y nadie más puede ver. La confidencialidad es distinguible

de la intimidad en el sentido de que "confidencial" implica el acceso a un conjunto de datos de muchas fuentes, mientras que "privado" por lo general significa que los datos sólo se pueden acceder a una única fuente. A modo de ejemplo, una contraseña se considera privada porque sólo una persona debe saber que, mientras que un archivo de historias clínicas se considera confidencial porque varios miembros del personal médico del paciente se les permiten ver.

• Integridad: Protección contra la modificación inadecuada de información o destrucción, incluida la garantía de no repudio de la información y la autenticidad. Una pérdida de integridad es la modificación o destrucción de información no autorizada.

La Integridad es particularmente relevante para los datos, se refiere a la seguridad de que los datos no han sido alterados de una manera no autorizada. Controles de integridad tienen el propósito de asegurar que un conjunto de datos no se puede modificar (o suprimir totalmente) por una parte no autorizada. Parte del objetivo de los controles de integridad es bloquear la capacidad de las personas autorizadas para realizar cambios en los datos, y otra parte es proporcionar un medio de restauración de los datos de nuevo a un estado bueno conocido (como en las copias de seguridad).

• Disponibilidad: Garantizar el acceso oportuno y confiable y uso de información. Una pérdida de disponibilidad es la interrupción del acceso o uso de información o un sistema de información.

A diferencia de la confidencialidad y la integridad, que hacen más sentido en el contexto de los datos contenidos en los sistemas informáticos, la disponibilidad se refiere al "tiempo de actividad" de los servicios de la seguridad basado en computadora que el servicio estará disponible cuando se necesita. La disponibilidad del servicio está generalmente protegida mediante la implementación de alta disponibilidad (o de servicio continuo) controles en las computadoras, redes y almacenamiento. De alta disponibilidad (HA) pares o grupos de computadoras, conexiones de red redundantes y discos RAID son ejemplos de mecanismos de protección de la disponibilidad. [20]

[20] Cengage Learning. Introduction to Information Security [En línea].
http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf

4.7.2 Establecimiento de un Sistema de Seguridad: Para afrontar el establecimiento de un sistema de seguridad en necesario conocer:

• Cuáles son los **elementos** que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
• Cuáles son los **peligros** que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.
• Cuáles son las **medidas** que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible. Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico, revisando y actualizando las medidas adoptadas.[21]

4.7.3 Norma ISO 31000: 2011 – Gestión de Riesgo: Esta norma es una guía importante al momento de gestionar los riesgos en toda organización, la cual brinda principios y directrices genéricas sobre la gestión del riesgo para ser utilizada por empresas públicas y privadas.

El proceso o esquema presentado por la norma, para la gestión del riesgo la guía se describen las actividades que comprenden el proceso de análisis de riesgo, con el desarrollo de los siguientes elementos: [22]

- Establecer el contexto
- Identificación del riesgo
- Análisis del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo
- Monitoreo y revisión
- Comunicación y consulta

[21] Purificación Aguilera. Seguridad Informática, 2010 Editex

[22] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN Trabajos escritos: presentaciones y referencias bibliográficas. NTC-ISO31000.Bogotá D.C. ICONTEC, 2011

4.8 LA EMPRESA DE TELECOMUNICACIONES Y SU MESA DE AYUDA PARA GRANDES CLIENTES

Dentro del área encargada de servicio a l cliente se encuentra el área de Soporte Empresarial o Mesa de ayuda para Grandes clientes, la cual tiene los siguientes objetivos:

- Ingresar los requerimientos del cliente a los aplicativos de gestión corporativos de la Empresa de Telecomunicaciones.
- Identificar el impacto de la falla presentada al cliente.
- Realizar pruebas de primer nivel de monitoreo de servicios.
- Escalar a las áreas que corresponda en el segundo nivel, para desarrollar las acciones correctivas.
- Realizar seguimiento a las actividades de escalamiento interno.
- Identificar la fuente del problema y solucionarlo.
- Comunicar al cliente los resultados de la gestión en curso.
- Confirmar con el cliente la normalización del servicio.
- Brindar asesoría integral al cliente.

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

El tipo de investigación que orienta el presente trabajo es de naturaleza descriptiva en consideración a que describe las características de la mesa de ayuda de la Empresa de Telecomunicaciones en su operación actual, y de naturaleza explicativa, al dar cuenta de las consideraciones argumentativas que justifican y responden la pregunta del planteamiento del problema, y hacen viable la transición a la modalidad de teletrabajo en condiciones seguras, de disponibilidad, confidencialidad e integridad.

Para tal propósito utiliza un enfoque mixto y complementario de técnicas de investigación, en primera instancia, respecto de su aplicación se apoya en la observación, la revisión bibliográfica de los conceptos asociados a teletrabajo y seguridad, y la revisión documental. En segunda, se apoya en la aplicación de técnicas como la entrevista, la realización de la identificación y calificación de los riesgos de seguridad que conlleva el cambio de modalidad de trabajo, y finalmente, se fundamenta en la conveniencia de realizar dicha transición apoyada desde el estudio y análisis de costos.

5.2 CARACTERIZACIÓN POBLACIÓN OBJETO DE ESTUDIO

La población objeto de estudio del presente trabajo la constituye la mesa de ayuda de Grandes Clientes de la Empresa de Telecomunicaciones. La naturaleza de estos clientes exige un tratamiento prioritario con la observancia de altos niveles de servicio, esto en consideración a que sus servicios críticos de negocio se encuentran soportados con tecnología de la Empresa de Telecomunicaciones. Al ser esta una empresa industrial y comercial del gobierno distrital encuentra jurisdicción en el Distrito Capital de la ciudad de Bogotá, en particular la mesa de ayuda.

Para las empresas denominadas como grandes clientes se ha creado la mesa de ayuda para los mismos", cuyo principal propósito es brindar soporte técnico de primer nivel a estos clientes, mediante un equipo de Ingenieros responsable de atender y dar respuesta a los requerimientos de los clientes.

El universo potencial susceptible de ser orientado a la modalidad de teletrabajo lo constituye un equipo de 38 Ingenieros, 7 analistas, 7 agentes de correo, y 9 agentes ADSL, sin embargo, en una primera fase, la propuesta de seguridad para teletrabajo desarrollada en este proyecto, considera como perfil de teletrabajadores el personal que maneja requerimientos y brindan atención al cliente en horario 7x24, es decir, un equipo de 30 Ingenieros que manejan los segmentos de empresas, en donde cada ingeniero tiene asignado cierto número de clientes a los cuales es necesario brindar atención en horario no hábil, para lo cual se realizan turnos.

5.3 TÉCNICA DE INVESTIGACIÓN E INSTRUMENTOS DE RECOPILACIÓN DE INFORMACIÓN

Entre las técnicas de investigación aplicadas como instrumentos de apoyo metodológico al presente trabajo se encuentran las siguientes:

La observación: Esta técnica se fundamenta, y encuentra contexto en el tipo de investigación descriptivo seleccionado, y se realiza desde la perspectiva de una de las autoras del presente trabajo, quien a su vez se encuentra vinculada con la Empresa de Telecomunicaciones en condición de Ingeniero de Soporte con cinco años de experiencia en procesos misionales, y para el desarrollo de esta técnica, desde el interior ha observado el modelo de servicio de la Empresa de Telecomunicaciones y frente al mismo, ha identificado como proceso susceptible de orientarlo a la modalidad de teletrabajo en condiciones del sistema de gestión de seguridad de la información, uno de sus elementos estructurantes como lo es la mesa de ayuda.

Revisión conceptual de teletrabajo y seguridad: como condición previa a la aplicación de la técnica anteriormente mencionada, se hizo necesario el apoyo en la revisión bibliográfica de los conceptos asociados a teletrabajo, los modelos de seguridad, y la seguridad aplicada al teletrabajo, los cuales han sido desarrollados ampliamente en el marco teórico a partir de la revisión en libros, normas técnicas e información tomada de internet, desde su dimensión histórica al nivel general (enfoque internacional), y al nivel específico (en Colombia), su dimensión conceptual, y legal. Del mismo modo, en la referencia de estos conceptos se encuentra una asociación de los mismos, elemento esencial como pilar de apoyo en la estructuración de la estrategia de seguridad que debe observar la transición a la modalidad de teletrabajo de la mesa de ayuda observada metodológicamente.

Revisión documental: En la aplicación de esta técnica se abordó inicialmente el sistema de gestión de calidad de la Empresa de Telecomunicaciones, en particular el mapa de procesos que representa gráfica y documentalmente, la relación entre los procesos de dirección, de apoyo, de seguimiento y evaluación con los procesos misionales de la Empresa de Telecomunicaciones, y es precisamente, en uno de estos procesos, como lo es el de Atención al Cliente, en donde se centra el estudio de viabilidad de orientación a la modalidad de teletrabajo.

Acto seguido, se realizó la referencia documental a todos los productos que ofrece la Empresa de Telecomunicaciones a sus clientes, a la descripción del Datacenter, a la infraestructura y desarrollo de las telecomunicaciones y conectividad remota, a la política y sistema de gestión de la seguridad de la información, y a los demás aspectos tecnológicos asociados al objeto de estudio del presente trabajo desarrollados en el capítulo No.6 “Desarrollo, resultados y aportes”.

Y es precisamente en este contexto referenciado, en donde se desarrollará la propuesta de seguridad de volcar a la modalidad de teletrabajo el proceso con el perfil de equipo analizado.

La entrevista: Dado que la observación y la referencia documental como técnicas de investigación son insuficientes para derivar conclusiones y recomendaciones sobre el particular, se acudió a otra técnica complementaria como la es la entrevista estructurada a partir de una serie de preguntas. Apoyada en las fuentes primarias y secundarias, que para el caso la constituyen el personal encargado de trámites y adquisición de recursos tecnológicos del área de Mesa de Ayuda.

Las preguntas se orientaron a establecer las condiciones estructurales, operacionales, económicas, de recurso humano, y apoyo al cumplimiento de las leyes, programas y planes, que hicieran posible orientar la mesa de ayuda a la modalidad de teletrabajo.

A continuación se presenta el cuestionario de preguntas utilizado en la entrevista al área en mención, a saber:

Respecto de las generalidades de proceso y/o procedimiento por orientar al teletrabajo:

- ¿Considera que el teletrabajo genera beneficios a las partes involucradas en el contrato?
- ¿Del modelo de servicio y asistencia al cliente de la Empresa de Telecomunicaciones cuál proceso y/o procedimiento es susceptible de orientar a la modalidad de teletrabajo?
- ¿Cuáles son los cargos, roles y perfiles del proceso y/o procedimiento seleccionado para orientar a la modalidad de teletrabajo?
- ¿Cuáles sistemas de la Empresa de Telecomunicaciones apoyarían instrumentalmente la operación del teletrabajador?
- ¿La Empresa de Telecomunicaciones dispone de recursos que permitan orientar el proceso perfilado por seleccionar al teletrabajo?
- Respecto del proceso y/o procedimiento del modelo de servicio y asistencia al cliente de la Empresa de Telecomunicaciones seleccionado.
- ¿Qué mecanismos de seguridad de la información tiene su operación actual?
- ¿Qué nivel de seguridad se requeriría para acceder remotamente en condiciones seguras? Esta pregunta se realiza con el objeto de fijar línea base.
- ¿Se logran los objetivos y metas respecto del proceso y/o procedimiento?
- ¿Los trabajadores del proceso y/o procedimiento cumplen con los horarios laborales?
- ¿La Empresa de Telecomunicaciones tiene flexibilidad respecto de las necesidades de sus trabajadores?

Identificación y calificación de los riesgos de seguridad: Del mismo modo, se acudió a otra técnica complementaria como la es la administración de riesgos en su fase de identificación y valoración de los riesgos del proceso /o procedimiento de la mesa de ayuda para Grandes Clientes. Esta técnica permite advertir los riesgos en seguridad evidenciados respecto de la operación actual y se realiza con el objeto de fijar línea base, al momento de proyectar aquellos que se encuentren presentes al orientar este proceso a la modalidad del teletrabajo.

5.4 PROCESAMIENTO Y ANÁLISIS DE DATOS

5.4.1 Análisis de observación, revisión conceptual y revisión documental: Utilizando la hipótesis y/o pregunta formulada en el planteamiento del problema del presente trabajo como punto de partida, direccionada a establecer la estrategia más efectiva de seguridad de la información por aplicar, al momento de decidir por parte del nivel directivo de la Empresa de Telecomunicaciones, sobre cuál de sus procesos misionales es susceptible de trasladar a la modalidad de teletrabajo, el abordaje metodológico se fundamentó en la aplicación de la observación, la

revisión conceptual, bibliográfica y documental, esta última con énfasis contextual en la Empresa de Telecomunicaciones.

Precisa señalar que la aplicación de estas técnicas no se realizó de manera secuencial e independiente, sino que obedeció a la aplicación en simultánea de las mismas; es decir, el marco conceptual proveyó las elementos teóricos y conceptuales de teletrabajo y seguridad, que aunados a la revisión documental referida específicamente a la Empresa de Telecomunicaciones, permitió mediante la observación realizar una revisión general de sus procesos.

De esta revisión se pudo constatar que existía una iniciativa al interior de la organización de orientar un proceso a la modalidad de teletrabajo, como fue la identificación de la mesa de ayuda como proceso. Es de señalar igualmente, que para las autoras de este trabajo, se tuvo la oportunidad de realizar esta constatación desde adentro de la organización, no sólo en condición de observadora por parte de una de sus integrantes, sino también con rol y juicio de experto, y en condición de responsable de ejecución de uno de sus procesos, como lo es el soporte, en esta organización.

En específico, de la aplicación simultánea de estas técnicas se logró establecer que esta iniciativa partió de la mesa de ayuda en condición de un piloto, el cual perseguía obtener los beneficios inherentes al teletrabajo; sin embargo, esta iniciativa se vio truncada por dos razones fundamentales, la primera referida a los cuestionamientos, preguntas e inquietudes que surgieron al momento de trasladar la mesa de ayuda del piloto a la modalidad de teletrabajo por los posibles riesgos y amenazas en seguridad, elementos estos, advertidos de manera preliminar, a priori y asistemática, y el segundo, por cuanto no obedecía a la ejecución de un plan operativo institucional para la mesa de ayuda formulado en este sentido por la organización.

Si bien es cierto, la aplicación de estas técnicas permitió perfilar el objeto y alcance de estudio del presente trabajo, también lo es que resultan insuficientes en cuanto a su propósito, y dicha situación exigió la aplicación de las técnicas complementarias que mencionan en la siguiente sección.

5.4.2 Análisis de los resultados de la entrevista: La entrevista estructurada definida en las técnicas de investigación fue aplicada al Coordinador de la Mesa de Ayuda de la Empresa de Telecomunicaciones, como responsable de los

procesos de soporte a los clientes de la Empresa de Telecomunicaciones, en particular, a los grandes clientes.

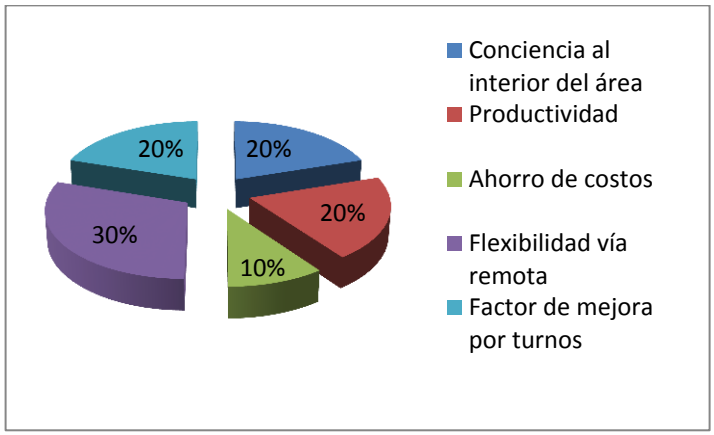
Su propósito esencial consistió en ratificar, de primera mano (en fuente primaria), las conclusiones preliminares y parciales identificadas, observadas y referenciadas con la aplicación de las técnicas antes desarrolladas, respecto de la condición de orientar la mesa de ayuda a la modalidad de teletrabajo. Igualmente, perseguía constatar que la Empresa de Telecomunicaciones cuenta con las condiciones estructurales, operacionales, económicas, de recurso humano, marco normativo, y plataforma estratégica y operativa propicias.

Para efectos ilustrativos se representan gráficamente las respuestas dadas por el entrevistado. Sobre el particular es de señalar, que la aplicación del instrumento (entrevista estructurada), al estar caracterizada por preguntas abiertas, se identifica una relación de entrevistado (responsable mesa de ayuda grandes clientes) a preguntas abiertas, y respecto de cada pregunta se identifican algunas variables, las cuales se expresan en porcentajes a partir del énfasis, reiteración y/o consideración especial o no por parte del entrevistado.

En tal sentido, al procesar y analizar las respuestas a las preguntas de la entrevista estructurada respecto de las generalidades del proceso y/o procedimiento por orientar al teletrabajo, se obtienen los siguientes resultados:

1. ¿Considera que el teletrabajo genera beneficios a las partes involucradas en el contrato?

Gráfica 1. Pregunta 1 entrevista teletrabajo

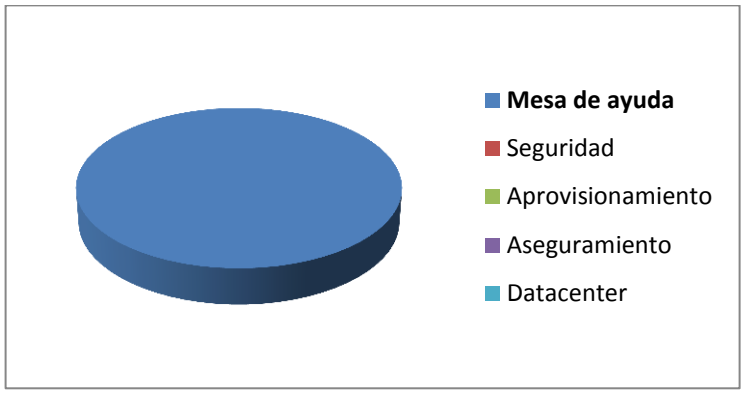


Fuente: Autores

Frente a la pregunta ¿Considera que el teletrabajo genera beneficios a las partes involucradas en el contrato?, el responsable del proceso manifiesta que sobre la modalidad de teletrabajo existe conciencia al interior del área, por cuanto en su momento fue considerada como una alternativa con importantes beneficios identificados en términos de productividad, ahorro de costos, y como un posible factor que mejora la relación contractual en circunstancias en donde la labor se puede trasladar al teletrabajo, se trabaja por turnos (como es el caso de la mesa de ayuda), y la flexibilidad que ofrece para ejecutarlo vía remota, es advertida como una variable positiva por los trabajadores, ya conocedores de sus beneficios.

2. ¿Del modelo de servicio y asistencia al cliente de la Empresa de Telecomunicaciones cuál proceso y/o procedimiento es susceptible de orientar a la modalidad de teletrabajo?

Gráfica 2. Pregunta 2 entrevista teletrabajo

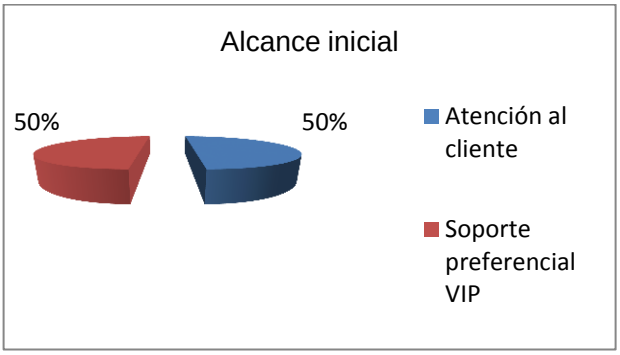


Fuente: Autores

A la pregunta ¿Del modelo de servicio y asistencia al cliente de la Empresa de Telecomunicaciones cuál proceso y/o procedimiento es susceptible de orientar a la modalidad de teletrabajo?, la respuesta ratifica a la mesa de ayuda como el proceso susceptible de trasladar a esta modalidad. De hecho la mesa de ayuda ha realizado una prueba piloto con 4 ingenieros del área que manejan clientes especiales, cuyos resultados identificaron viabilidad en esa orientación; sin embargo, por la ausencia de establecimiento de políticas de seguridad para la conexión remota y el manejo seguro de la información en el área de Mesa de Ayuda, esta iniciativa no se instituyó como forma de trabajo para todos los ingenieros del área.

3. ¿Cuáles son los cargos, roles y perfiles del proceso y/o procedimiento seleccionado para orientar a la modalidad de teletrabajo?

Gráfica 3. Pregunta 3 entrevista teletrabajo

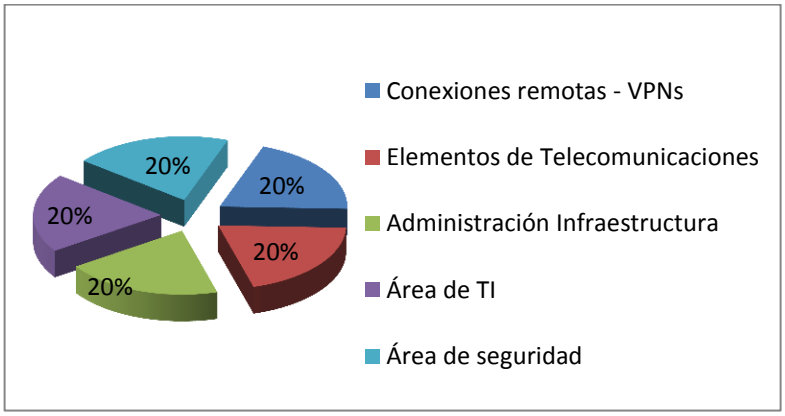


Fuente: Autores

Igual que la anterior, en relación con la pregunta ¿Cuáles son los cargos, roles y perfiles del proceso y/o procedimiento seleccionado para orientar a la modalidad de teletrabajo?, se responde que su alcance inicial estaría centrado en la mesa de ayuda encargada de la atención y soporte preferencial- VIP (Very Important Person por sus siglas en inglés) a clientes especiales, cuya atención se realiza 7x24. Se estaría hablando de un equipo de trabajo de 30 ingenieros de soporte de la mesa de ayuda.

4. ¿Cuáles sistemas de la Empresa de Telecomunicaciones apoyarían instrumentalmente la operación del teletrabajador?

Gráfica 4. Pregunta 4 entrevista teletrabajo

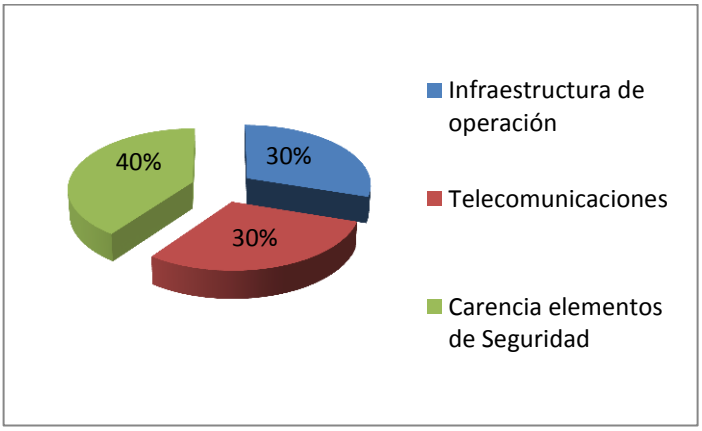


Fuente: Autores

A la pregunta ¿Cuáles sistemas de la Empresa de Telecomunicaciones apoyarían instrumentalmente la operación del teletrabajador? Se responde que la organización cuenta con la conexión y elementos de telecomunicaciones necesarios de base para Teletrabajo consistentes en la red corporativa, y las conexiones remotas que maneja, en este caso la VPNs (Virtual Private Net por sus siglas en inglés), administradas, gestionadas y salvaguardadas por el área de TI y Seguridad de la Empresa de Telecomunicaciones.

5. ¿La Empresa de Telecomunicaciones dispone de recursos que permitan orientar el proceso perfilado por seleccionar al teletrabajo?

Gráfica 5. Pregunta 5 entrevista teletrabajo

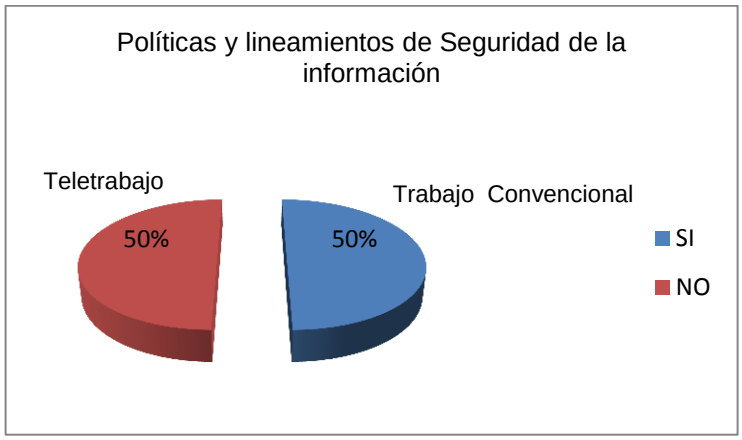


Fuente: Autores

Finalizando este bloque de preguntas genéricas relativas a los procesos susceptibles de trasladar al teletrabajo, se pregunta si ¿La Empresa de Telecomunicaciones dispone de recursos que permitan orientar el proceso perfilado por seleccionar al teletrabajo?, frente a la cual se responde que la infraestructura de operación y telecomunicaciones se encuentra provista y se constituye en un elemento estructural determinante que hace viable el proceso; sin embargo, se reitera que se debe resolver los elementos propios de seguridad de la información propios de su traslado a esta modalidad y recomendar a la alta dirección de la organización la propuesta que recoja estos elementos.

6. ¿Qué mecanismos de seguridad de la información tiene su operación actual?

Gráfica 6. Pregunta 6 entrevista teletrabajo

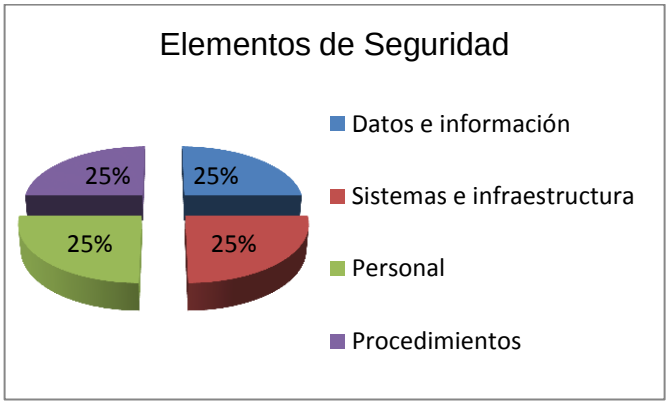


Fuente: Autores

Al revisar el proceso y/o procedimiento del modelo de servicio y asistencia al cliente de la Empresa de Telecomunicaciones seleccionado, en relación con la pregunta acerca de ¿Qué mecanismos de seguridad de la información tiene su operación actual? Se menciona que la entidad cuenta una política y lineamientos de seguridad de la información, los cuales se concretan en el sistema de gestión de la seguridad de la información que está orientado a todo el contexto de infraestructura y sistema de información cobijada por la red corporativa en la Empresa de Telecomunicaciones, se menciona igualmente que no existen lineamientos de seguridad específicos a la modalidad de teletrabajo en razón de que no existe un proceso con desempeño en esa modalidad.

7. ¿Qué nivel de seguridad se requeriría para acceder remotamente en condiciones seguras?

Gráfica 7. Pregunta 7 entrevista teletrabajo

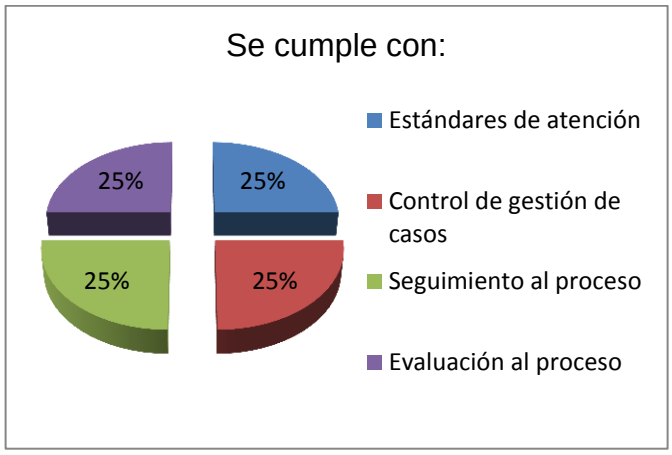


Fuente: Autores

A la pregunta sobre ¿Qué nivel de seguridad se requeriría para acceder remotamente en condiciones seguras?, se manifiesta que los elementos de seguridad que ofrece el sistema de seguridad de la información de la Empresa de Telecomunicaciones; es decir, aquellos centrados sobre el radio de acción salvaguardados por la red corporativa.

8. ¿Se logran los objetivos y metas respecto del proceso y/o procedimiento?

Gráfica 8. Pregunta 8 entrevista teletrabajo



Fuente: Autores

Relativo a la pregunta ¿Se logran los objetivos y metas respecto del proceso y/o procedimiento?, se expresa por el responsable de la mesa de ayuda, que estos se cumplen conforme lo formulado, y en el margen de tolerancia previsto en los estándares de atención a los clientes especiales propios e inherentes al esquema de escalamiento y resolución de los incidentes. De hecho existe un control de gestión propio de la herramienta de Mesa de Ayuda que permite en la modalidad de gestor de casos, asignar los mismos, escalarlos, ver los tiempos de atención en cada fase y permite igualmente, la realización en consecuencia, de la trazabilidad frente a casos puntuales, no sin olvidar los mensajes de alerta que por defecto genera el sistema.

9. ¿Los trabajadores del proceso y/o procedimiento cumplen con los horarios laborales?

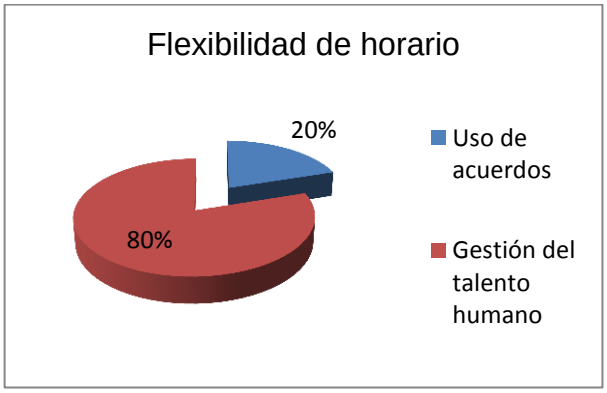
Gráfica 9. Pregunta 9 entrevista teletrabajo

Fuente: Autores

En relación con la pregunta, ¿Los trabajadores del proceso y/o procedimiento cumplen con los horarios laborales?, el responsable del área menciona que en efecto el horario se cumple a cabalidad, y que existen algunos eventos no representativos en su cumplimiento sobre todo en los turnos no hábiles; sin embargo, hace énfasis sobre la logística de transporte que realiza la Empresa de Telecomunicaciones, y la propia del equipo de soporte, en el desplazamiento de los ingenieros procedentes de diferentes localidades y sitios de Bogotá a la mesa de ayuda ubicada en Usaquén. Esta situación se simplificaría con la orientación hacia el teletrabajo.

10. ¿La Empresa de Telecomunicaciones tiene flexibilidad respecto de las necesidades de sus trabajadores?

Gráfica 10. Pregunta 10 entrevista teletrabajo



Fuente: Autores

Culminando este bloque con la pregunta ¿La Empresa de Telecomunicaciones tiene flexibilidad respecto de las necesidades de sus trabajadores?, el responsable contesta que si la pregunta es referida a la flexibilidad en el horario y en acometer ciertas tareas, la misma no obedece a una política y modelo de operación definido, sino más bien a situaciones independientes y aisladas que se acuerdan con los trabajadores en condiciones especiales y/o excepcionales. Es decir, respecto de algunas incapacidades, permisos y en definitiva situaciones particulares propias de la gestión del talento humano.

Finalmente, con la aplicación de esta técnica se logró confirmar el perfilamiento, foco y alcance de la propuesta en seguridad que respalda el presente trabajo, previamente advertidas con la aplicación de la observación, la revisión conceptual y documental sobre los elementos propios de teletrabajo de la mesa de ayuda orientado en condiciones seguras, disponibles, integras y confiables. Y del mismo modo, se logró identificar que la Empresa de Telecomunicaciones cuenta con las condiciones estructurales, operacionales, y de plataforma estratégica y operativa propicias que hace viable esta orientación.

5.4.3 Análisis de la Identificación y calificación de los riesgos de seguridad: Al realizar un análisis en la identificación de amenazas, vulnerabilidades e impacto, la organización posee un registro de su identificación actualmente, y con base en un contexto interno y externo en los que se consideran al gestionar los riesgos como es en el ambiente natural, humano, operacional, tecnológica, social, entre otros.

Con lo anteriormente mencionado, se realiza una búsqueda de las debilidades en el sistema de seguridad para su clasificación al momento de que se pueda presentar al trasladar la operación a la modalidad del teletrabajo.

De acuerdo a la información suministrada mediante la entrevista y el levantamiento del proceso de atención de reportes; las variables contempladas en la mesa de ayuda como valor para la organización, son: La información, Bases de datos, Recurso humano, Hardware y software propiedad de la organización.

En cuanto a la identificación de controles existentes en trabajo presencial, el actual procedimiento de controles que se tiene, para determinar su estado, permitiendo realizar un análisis detallado y complementación para su posterior aplicación a teletrabajo.

En el análisis y calificación de riesgos, identificados al momento de trasladar la operación a la modalidad del teletrabajo, se calcula el impacto, la probabilidad de ocurrencia y el nivel de riesgo. El análisis de riesgo, considera la identificación de los activos, de acuerdo a su nivel de importancia, asignando valores de estimación de riesgo, con un impacto y probabilidad en cada caso y los valores serán cualitativos o cuantitativos.

6. LEVANTAMIENTO DE INFORMACIÓN Y RECOLECCIÓN DE DATOS

Antes de realizar el desarrollo de la propuesta, resultados, y aportes del presente capítulo, se hace necesario conocer una breve reseña y caracterización de los productos que ofrece la Empresa de Telecomunicaciones, lo cual permitirá tener un contextualización específica del entorno en donde se planteará y desarrollará la propuesta, a saber:

6.1 CARACTERIZACIÓN DE PRODUCTOS

Los productos ofrecidos por la Empresa de Telecomunicaciones son:

6.1.1 Voz: La Empresa de Telecomunicaciones cuenta con una red de telefonía local a través de la que se ofrecen servicios de: Líneas telefónicas, servicio de PBX, enlaces de voz local, enlaces de voz local IP y servicios suplementarios sobre los servicios de telefonía local.

Larga Distancia: La Empresa de Telecomunicaciones cuenta con cobertura nacional e internacional para llamadas de larga distancia marcando desde líneas nacionales. Los servicios de Larga Distancia son: Discado directo nacional e internacional; acuerdos de voz de larga distancia corporativos; tarjeta post pago, para usuarios con requerimientos de movilidad nacional e internacional

Telefonía Local: La Empresa de Telecomunicaciones ofrece servicios de: Líneas telefónicas, servicio de PBX, enlaces de voz local, enlaces de voz local IP y servicios suplementarios sobre los servicios de telefonía local.

Comunicaciones administradas IP – IP Centrex: Servicios de Telefonía IP, como IP Centrex.

Servicios de Red Inteligente: Oferta de servicios de numeración especial para líneas de atención o servicios de información.

6.1.2 Internet: Los servicios de Internet ofrecidos son: Banda Ancha, Internet Dedicado, Internet Fibra Óptica e Internet Banda Ancha, los cuáles con descritos a continuación:

Banda Ancha: Servicio que permite ofrecer accesos a Internet, empleando tecnología

Internet Dedicado: Servicio que emplea las tecnologías de acceso y transporte de la red de Conectividad Avanzada IP de la Empresa de Telecomunicaciones para ofrecer enlaces permanentes y exclusivos, con anchos de banda simétricos garantizados.

Internet Fibra Óptica: Servicio prestado a través de la red de fibra óptica cuyas diferencias tecnológicas, permiten velocidades muy superiores a las ofrecidas por banda ancha

Internet Banda Ancha: Este servicio de acceso dedicado a Internet, le permite a las empresas tener una conexión permanente y exclusiva con anchos de banda garantizados para aplicaciones de negocio no críticas.

6.1.3 Datos: La empresa cuenta con soluciones de datos que consisten en Servicio Portador y Conectividad Avanzada cuya definición es:

Servicio Potador: Servicio que permite a las empresas resolver necesidades de: transporte de datos, voz y video entre oficinas; interconexión con Centrales de Conmutación, Troncales o PBX; transporte de grandes capacidades de información.

Conectividad Avanzada: Es el servicio por medio del cual las empresas pueden adquirir una solución integral de comunicación de datos con tecnología de punta, para resolver necesidades en conectividad fija, conectividad móvil y conectividad avanzada IP.

6.1.4 Data Center: La Empresa de Telecomunicaciones brinda a sus clientes los siguientes servicios Data Center:

Recuperación Ante Desastres Y Continuidad De Negocio: Servicio que permite a las empresas disponer de un plan de contingencia ante eventualidades que puedan afectar la continuidad del negocio

Colocación: Es el servicio que permite ofrecer al cliente el área o unidades de rack dentro de los Data Center de la Empresa de Telecomunicaciones para situar los servidores y equipos de comunicación que soportan la operación del negocio.

Hosting Dedicado: Alojamiento de aplicaciones de cliente en servidores exclusivos suministrados y administrados por la Empresa de Telecomunicaciones en la red de Data Centers. Los clientes pueden acceder a sus aplicaciones o servidores por medio de servicios de conectividad que pueden ser suministrados de igual manera por la Empresa de Telecomunicaciones.

Hosting Compartido: Alojamiento y almacenamiento de información de clientes en instancias compartidas independientes de servidores de la Empresa de Telecomunicaciones, garantizando los recursos de cómputo por cada instancia. Estos servidores pueden almacenar páginas web, bases de datos y casillas de correo electrónico.

Hosting De Correo Electrónico: Este servicio permite en las empresas que sus colaboradores puedan tener servicio de correo electrónico corporativo, robusto y eficiente. Adicionalmente, este servicio permite todas las funcionalidades de correo estándar, avanzadas y de mensajería; siendo estas administradas directamente por el cliente de acuerdo a sus políticas.

Hosting de Mensajería y Colaboración: Consiste en ofrecer un servicio de colaboración intermedia (chat, conferencias, videoconferencia, y otras herramientas de colaboración) entre usuarios del dominio de la compañía o fuera de ella.

Almacenamiento en la Nube: El servicio de almacenamiento remoto permite que una empresa que cuenta con servidores en sus premisas pueda almacenar sus datos en una plataforma de alto rango, con alta disponibilidad de la data y con la seguridad que entregan las plataformas de almacenamiento ubicadas en la Nube de la Empresa de Telecomunicaciones.

Hosting Virtual: Es una solución de servicios de Hosting Dedicado soportado por una robusta plataforma alistada para prestación de servicios en la Nube que permite asignar recursos informáticos a los clientes

Base de Datos como Servicio: Es un servicio bajo demanda, orientado a un esquema de base de datos en la Nube de la Empresa de Telecomunicaciones donde se entrega el motor de base de datos en una o varias instancias virtuales, con las características requeridas por el cliente, suministrando: criterios de aislamiento, alta disponibilidad de la Nube de la Empresa de Telecomunicaciones y Monitoreo de sus bases de Datos.

Backup en la Nube: Este servicio consiste en una solución de backup a la Nube aplicable a cualquier tipo de empresa con herramientas avanzadas para respaldo de aplicaciones, bases de datos, hipervisores y archivos Es una solución que incluye todas las herramientas y funciones que las empresas necesitan hoy en día para manejar sus datos distribuidos desde la Nube de la Empresa de Telecomunicaciones, con seguridad, confiabilidad y eficiencia.

Reportes de Análisis de Vulnerabilidades: Es un servicio en la Red de Data Centers de la Empresa de Telecomunicaciones que diagnostica y defiende los servicios de Tecnologías de Información (TI) frente a amenazas diarias dadas por hackers, filtraciones de datos, software publicitario, spyware y ventanas emergentes, entre otros.

6.2 PROCESOS DE SOPORTE A GRANDES CLIENTES

Foco específico

Cuando un cliente contrata uno de los servicios anteriormente mencionados, la Empresa de Telecomunicaciones debe garantizar el correcto aprovisionamiento y el aseguramiento del mismo. El aprovisionamiento consiste en la etapa de diseño, implementación y puesta en marcha del servicio solicitado y el aseguramiento, en mantener el correcto funcionamiento del servicio las 24 horas y los 365 días del año brindando soporte técnico y determinados tiempos de solución cuando se presenten problemas.

Existe una serie de clientes que requieren mayor atención y prioridad debido a que se trata de grandes empresas con servicios críticos para su negocio soportados con tecnología de la Empresa de Telecomunicaciones. Para este tipo de clientes se crea la mesa de ayuda de grandes clientes, esta área brinda soporte técnico de primer nivel al cliente, a través de Ingenieros encargados de atender y dar respuesta a los requerimientos de los clientes; esta área cuenta actualmente con 38 Ingenieros, 7 analistas, 7 agentes de correo, 9 agentes ADSL (Asymetric Digital Subscriber Line por sus siglas en Inglés), la propuesta de seguridad para teletrabajo que se desarrolla en este proyecto estará dirigida hacia el personal que maneja requerimientos y brindan atención al cliente en horario 7x24

Para el propósito anteriormente mencionado, inicialmente se investiga y documentan los procesos, requerimientos y herramientas actuales, necesarias para que cada ingeniero realice su labor de forma eficiente

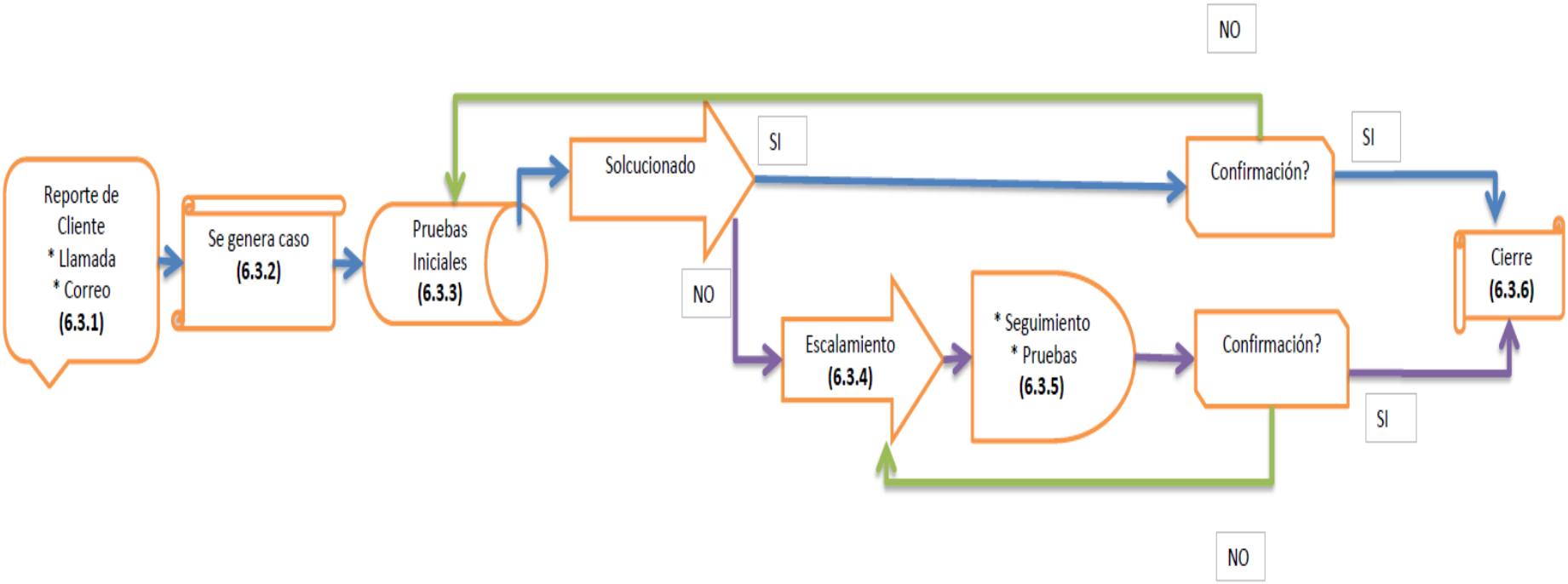
En esa línea, para garantizar la atención y respuesta permanente a los clientes, la Empresa de Telecomunicaciones ofrece un centro de gestión y servicio de soporte a fallas que opera 24 horas del día, los 365 días del año (atención 7x24)

La mesa de ayuda cuenta con un grupo de operadores para dar solución a los problemas que pueda tener el cliente, apoyados con herramientas de software que suministran toda la información acerca del estado de los servicios.

6.3 DESCRIPCIÓN DEL PROCESO DEL REPORTE DE CLIENTE

Inicialmente y de forma general se tiene el proceso de atención de reportes que se observa en la Figura 3, en donde se puede ver el flujo de trabajo básico previsto para gestionar los casos que se presentan en la mesa de ayuda con el correspondiente escalamiento en los niveles de servicio. El mismo se constituye en un elemento de referencia al momento de advertir en donde se identificarán los riesgos al orientarlo a la modalidad de teletrabajo y en donde deben estar presentes los controles

Figura 3. Proceso de atención de reportes



Fuente: Autores

6.3.1 Reporte del Cliente: El punto de contacto entre la Empresa de Telecomunicaciones y el cliente, en lo que a soporte y posventa se refiere, se realiza a través del Centro de Soporte Empresarial. A través de esta línea el cliente debe reportar sus peticiones, solicitudes y reclamos. Los ingenieros que reciben la llamada de servicio son los interlocutores con el cliente para la evolución, resolución y cierre de la llamada de servicio. Una vez abierto un caso, se asigna un número de tiquete para seguimiento.Como medio alternativo de contacto, los clientes podrán dirigir sus requerimientos de servicio, relacionados con fallas técnicas de la solución, vía correo

En caso de incidente o necesidad de soporte técnico, el cliente se deberá comunicar al Call Center de número del Centro de Soporte Empresarial asignado de acuerdo con su segmento, y debe reportar los siguientes aspectos:

- Hora del incidente
- Descripción del incidente
- Mensaje de Error (Si aplica)

Posteriormente se asignará un tiquete de atención, el cual podrá ser utilizado por el cliente para hacer seguimiento a su orden de servicio. El tiempo de atención y el proceso de escalar incidentes se basará en el nivel de prioridad de la falla, que se establece de acuerdo al impacto que genere en el negocio como se observa en el Cuadro 1:

Cuadro 1. Nivel de prioridad

Nivel de prioridad de la falla	Tipo de falla
1	**Alta**: “Afecta considerablemente el negocio”. Ejemplo: Perdida total del servicio y no existe una solución alterna
2	**Media**: “Degradación del servicio; 25-50% sin servicio”. Ejemplo: Una parte importante del servicio está abajo.
3	**Baja**: “Requerimientos y/o Dificultad para trabajar que no compromete la disponibilidad ni el desempeño del servicio.”

Fuente: Fuente: Empresa de Telecomunicaciones

Teniendo en cuenta el impacto de la falla y la prioridad asignada al incidente, los tiempos de diagnóstico y solución de fallas son:

Cuadro 2. Prioridad del incidente

Prioridad del incidente	**Horario**	**Atención Dd hh:mm:ss**	**Diagnóstico Dd hh:mm:ss**
Alta	7X24	00 01:00:00	00 04:00:00
Media	7X24	00 02:00:00	00 08:00:00
Baja	Lunes a Viernes de 8:00am a 5:00pm	00 04:00:00	00 12:00:00

Fuente: Empresa de Telecomunicaciones

6.3.2 Generación de caso: Este paso es realizado en la herramienta de gestión de reportes de la Empresa de Telecomunicaciones:

- Se ingresa el registro del requerimiento, con el fin de documentar el caso, hacer seguimiento a los tiempos de respuesta y expedir un ticket o un radicado según el canal de donde provenga el requerimiento.
- De acuerdo con la tipología y tipo de producto, el sistema automáticamente enruta el requerimiento de soporte técnico al canal correspondiente

6.3.3 Pruebas Iniciales: Este paso se realiza posteriormente al recibir el caso, registrado en la herramienta de gestión de reportes de la Empresa de Telecomunicaciones, se procede a:

- Con base en la información recopilada sobre los inconvenientes que el cliente ha detectado en el servicio y demás información requerida se determina si la causa es común o no (masiva).
- Ejecutar las pruebas correspondientes al diagnóstico efectuado, para asi buscar las soluciones. Se utilizan las herramientas de gestión y monitoreo disponibles.
- De acuerdo con el resultado arrojado por las pruebas, se efectuan las accciones determinadas para cada caso y se verifica si el servicio se restableció.
- Apoyado en el analisis de la información arrojada por las pruebas iniciales, definir cual es la causa del problema que reporta el cliente.
- El cliente debe tener claros los motivos por los cuales se le pueden haber presentado situaciones inusuales con su servicio, para así poder remediarlos.

6.3.4 Escalamiento del reporte: Después de realizar las pruebas correspondientes el Ingeniero determinará si le es posible solucionar la falla o dar respuesta al requerimiento del cliente, o si es necesaria la colaboración por parte de áreas especializadas de la empresa, si es así y dependiendo del tipo de falla o requerimiento se enrutará hacia el área respectiva mediante la asignación del reporte generado en la herramienta de gestión al grupo o usuario a quien corresponda la solución de dicha falla.

Por parte del Ing. de soporte responsable inicial del caso, se realizarán los seguimientos y escalamientos respectivos para dar solución y respuesta al cliente dentro de los tiempos determinados.

6.3.5 Seguimiento: Este paso es fundamental, dado a su objetivo de evaluación y calidad del servicio. A continuación se detalla la forma de realizarlos.

- Se informa al cliente la razón por la cual ha tenido inconvenientes en el servicio y el tiempo estimado de solución, teniendo en cuenta los acuerdos de niveles de servicio firmados con el cliente.
- Se registran detalladamente las acciones que se efectuaron durante la gestión, luego si se solucionó el caso se cierra el ticket correspondiente, si fué información por causa común este quedará abierto hasta que la falla sea solucionada y se procede a cerrar la llamada.
- Si el cliente lo requiere se puede generar un informe de la falla presentada, que será publicado en el portal e-services.

6.3.6 Confirmación y Cierre de reporte: Una vez se haya verificado con el cliente que la solución dada a la llamada de servicio cumple con los compromisos establecidos, el ingeniero del soporte procederá a cerrar la llamada y a documentarla en la herramienta de gestión de tiquetes técnicos.

6.4 TIPOS DE REPORTE Y HERRAMIENTAS REQUERIDAS

A continuación se presenta un cuadro de los tipos de reporte recibidos en la Mesa de Ayuda y las herramientas necesarias para gestionar los mismos:

Cuadro 3. Tipos de reportes

Herramienta	**Web**		**VPN**		**Móvil**
Reporte / Requiere	Acceso a aplicativo y seguimiento de reportes	Acceso a Correo	Gestión de equipos de Core o nodos centrales	Base de Datos de Clientes	Contacto Telefónico con cliente
Cambio de configuración	x	x	x	x	x
Daño enlace E1	x	x		x	x
Daño enlace PRI	x	x		x	x
Daño periféricos	x	x		x	x
Daño RDSI BRI	x	x		x	x
Daño red inteligente	x	x		x	x
Daño Cx	x	x		x	x
Datacenter	x	x		x	x
Enlace caído	x	x	x	x	x
Enlace hibrido	x	x	x	x	x
Falla de voz	x	x	x	x	x
Informativo	x	x		x	x
Intermitencias	x	x	x	x	x
Lentitud de internet	x	x	x	x	x
Lentitud enlace de datos	x	x	x	x	x
Mantenimiento	x	x		x	x
No navega	x	x	x	x	x
Perdida de paquetes	x	x	x	x	x
Problemas de correo	x	x		x	x
Problemas de hosting	x	x		x	x
Solicitud de informe	x	x		x	x

Fuente: Empresa de Telecomunicaciones

Una vez analizada y estudiada la información, la organización, los procesos realizados y las herramientas utilizadas por cada empleado en su trabajo presencial, con el objeto de que este personal cuente con los instrumentos mínimos necesarios para realizar su labor como si estuviera presente en la oficina, se procede a enlistar los requerimientos tecnológicos para Teletrabajo:

- Canal de Internet
- Acceso a aplicativo para registro y seguimiento de reportes (HP Service Manager)
- Acceso a Correo corporativo (Outlook web app)
- VPN (Gestión de equipos de Core Empresa de Telecomunicaciones o nodos centrales y Acceso a Base de Datos de Clientes) Solución de telefonía (Contacto Telefónico con cliente, seguimiento interno, escalamiento con otras áreas)

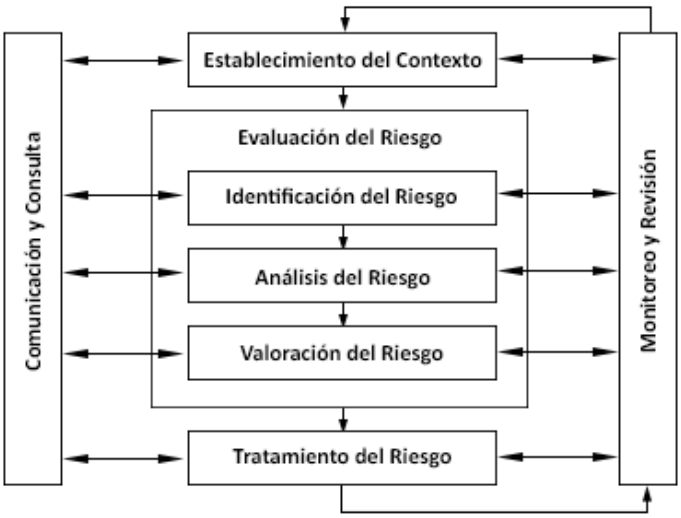
En entrevista realizada a uno de los coordinadores del área, se encuentra que algunos ingenieros de la mesa de ayuda que manejan clientes especiales que son también proveedores de tecnología y telecomunicaciones, han realizado jornadas laborales de Teletrabajo en horarios nocturnos ocasionalmente con herramientas adicionales brindadas por la Empresa de Telecomunicaciones para la realización del mismo.

En entrevista con uno de los ingenieros que ha realizado Teletrabajo, informa de las herramientas utilizadas y suministradas, como también el manejo de los procesos en esta modalidad de trabajo

- Canal de Internet: Propiedad del Ingeniero, en su lugar de residencia
- Ordenador: Propiedad del Ingeniero
- VPN: Check Point VPN suministrada por el área de seguridad de la Empresa de Telecomunicaciones
- Solución de telefonía Teléfono móvil: Propiedad del área de Mesa de Ayuda a donde se direccionan las llamadas de clientes y se establece comunicación con otras áreas
- Correo corporativo: asignado por la empresa vía web mail
- Acceso a herramienta de gestión de reportes: vía web HP Service Manager
- Acceso a Base de datos de clientes mediante una VPN Cisco Anyconnect

Basado en esta información se procedió a realizar un análisis de riesgos y propuesta de seguridad con el fin de dar confianza a los directivos, de cuáles la mejor estrategia de ampliar la modalidad de teletrabajo a toda el área de Mesa de Ayuda, y de esta manera establecerla como una forma de trabajo. En consecuencia, se procede a realizar el análisis de riesgo correspondiente basado en la norma ISO 31000: 2011.

Figura 4. Proceso para la gestión del riesgo



Fuente: INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN NTC-ISO 31000. Esquema del proceso de riesgos. Bogotá D.C. ICONTEC, 2011.

7. GESTIÓN DE RIESGO

Para el desarrollo de la propuesta ítem se describirá el paso a paso sugerido desde la norma, y se analizará en simultánea los resultados evidenciados, a saber:

7.1 ESTABLECIMIENTO DEL CONTEXTO

El primer paso para realizar gestión de riesgos según la norma ISO 31000: 2011 es establecer el contexto, en donde se tienen en cuenta los objetivos de la organización, se definen los parámetros a considerar para establecer el alcance, los criterios y como resultado la gestión de riesgos.

La gestión del riesgo se debe emprender con total consideración de la necesidad de justificar los recursos utilizados para llevar a cabo dicha gestión.

Para ello, basados en el levantamiento previo de la información y las entrevistas realizadas a personal directivo de la mesa de ayuda, se establecen los siguientes objetivos generales hacia donde se enfocan las actividades realizadas por los Ingenieros del área y que en caso de implementar Teletrabajo deben seguirse cumpliendo:

- Proteger la información de la Empresa de Telecomunicaciones

Debido a que cualquier acceso a los aplicativos o a los equipos de red de comunicaciones por parte de personal no autorizado, podría incurrir en fallas masivas que afectarían varios clientes, es importante salvaguardar la información de accesos y servicios

El ingreso a los equipos de Core o nodos centrales de Empresa de Telecomunicaciones por parte de personal no autorizado, podría repercutir en pérdidas de información, borrado de configuración y por ende afectación del servicio tanto de los clientes como de Empresa de Telecomunicaciones.

- Proteger la información de los clientes que viaja a través de la red y contenida en los servicios ofrecidos

La Empresa de Telecomunicaciones maneja diferentes tipos de cliente entre los cuales se encuentran entidades gubernamentales, financieras entre otros, que manejan información personal y confidencial tanto del negocio como de sus propios clientes, dicha información viaja o se trata a través de los servicios tecnológicos ofrecidos por la Empresa de Telecomunicaciones; por lo cual durante la realización de contratos comerciales con los clientes se firma además un contrato de confidencialidad de la información de parte y parte

El Ingeniero de soporte al cual aplica esta propuesta de seguridad en Teletrabajo, tiene acceso tanto a los equipos de Core o nodos centrales de en la Empresa de Telecomunicaciones, como a los equipos finales en los clientes, también a bases de datos en donde se encuentra información de contactos de TI de cada empresa cliente, direccionamiento IP, servicios, topología de red etc. que debe ser protegida

- Mantener los niveles de servicio con los clientes

Además de la seguridad de la información que viaja o se trata a través de la red de la Empresa de Telecomunicaciones, se debe velar por la calidad de servicio que se brinda al cliente en caso de un requerimiento o falla, es decir, disponibilidad de servicio, tiempos de respuesta y restablecimiento de servicio determinados según contrato, por lo cual es importante para el desempeño del Ingeniero de Soporte que las herramientas se encuentren activas y disponibles mientras realiza sus labores en modalidad de Teletrabajo

De allí se pueden derivar algunos objetivos específicos:

- Mejorar tiempos de respuesta a requerimientos y reportes
- Brindar información clara y confiable al cliente de los seguimientos y actividades realizadas para dar respuesta o solución al requerimiento
- Documentar todas las actividades realizadas en el reporte
- Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma
- Cumplir oportunamente con labores asignadas

- Mantener una comunicación e interacción eficaz con otras áreas especializadas

Se determinan igualmente varios procesos y las actividades realizadas en los mismos:

- Registro turno
  Inicio de Turno
  Finalización de Turno
- Reporte de Cliente
  Recepción de nuevos reportes
- Pruebas Iniciales
  Búsqueda de información de cliente y servicio reportado
  Pruebas de primer nivel
- Seguimiento
  Recepción de reportes para seguimiento al inicio de turno
  Seguimiento a reportes en herramienta de gestión
  Avances al cliente mediante correo
  Avances telefónicos al cliente
  Confirmación de operatividad con el cliente vía correo
  Confirmación de operatividad con el cliente telefónica
  Envío de reportes para seguimiento al finalizar el turno
- Escalamiento del reporte
  Escalamiento a otras áreas mediante correo
  Escalamiento telefónico a otras áreas

Teniendo en cuenta los objetivos mencionados se definen los posibles eventos que se podrían presentar:

- Malos tiempos de respuesta al cliente debido a problemas en la disponibilidad de los activos, o problemas de lentitud
- Información confusa o errónea al cliente debido a falta de integridad de la información que se maneja y problemas en la disponibilidad de elementos para la comunicación
- Falta de documentación y seguimiento de actividades realizadas debido a problemas en la disponibilidad de los activos
  - Revelación de información crítica de la Empresa de Telecomunicaciones o del cliente por falla en manejo de información confidencial
- Incumplimiento en labores asignadas debido a problemas en la disponibilidad de los activos

El área de mesa de ayuda para grandes clientes debe cumplir con niveles de servicio impuestos por la empresa, el incumplimiento de estos indicadores repercute en descuentos al presupuesto mensual:

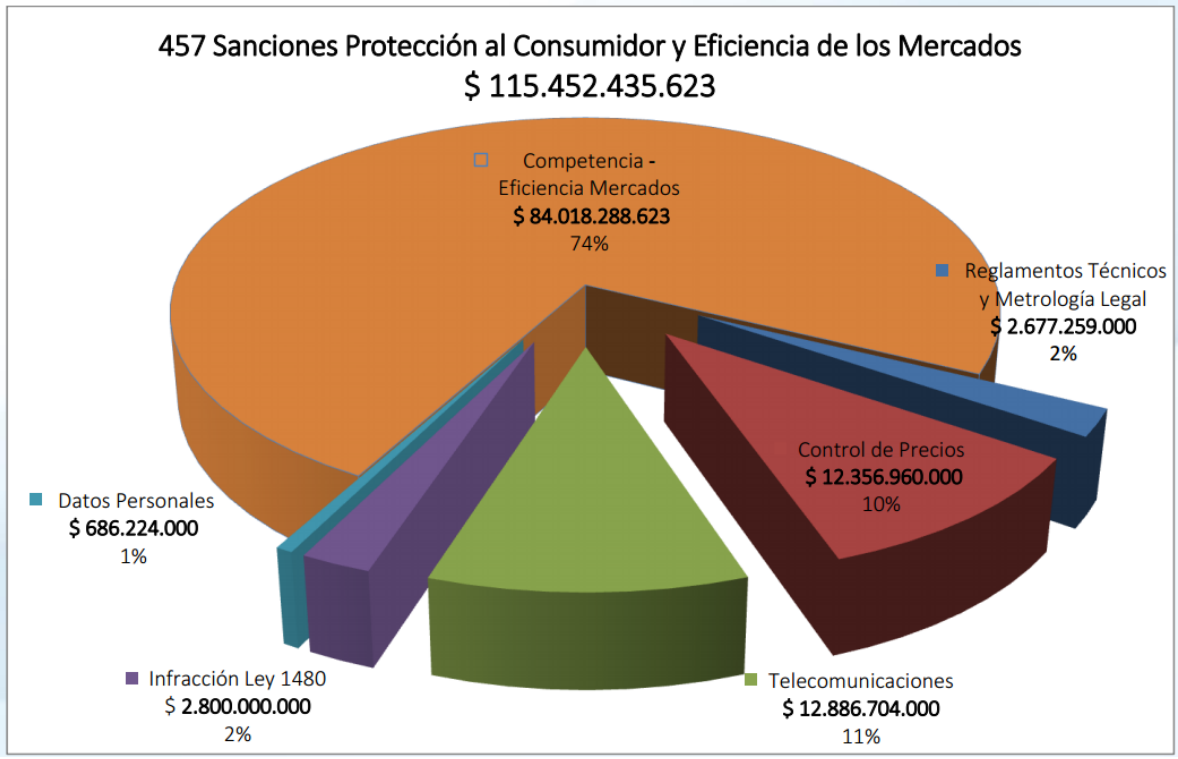
- Escalamiento, los casos generados en caso de requerir escalamiento se debe realizar el mismo en máximo 30 minutos después de la creación del reporte
- Primer nivel, los casos que pueden ser solucionados por el Ingeniero de mesa de ayuda deben ser cerrados antes de 8 horas hábiles
- Efectividad, los casos generados a los ingenieros de la mesa de ayuda deben ser cerrados en máximo 5 días
- Seguimiento, se debe mantener informados a los clientes de las avances de las actividades realizadas en cada caso y cada llamada debe registrarse como un seguimiento en el reporte generado

Se debe tener en cuenta que se manejan descuentos por indisponibilidad del servicio cuando por alguna razón no se cumple con la disponibilidad ofrecida para los servicios de Enlaces de Datos Dedicado y Enlaces de Internet Dedicado, la Empresa de Telecomunicaciones compensa económicamente al cliente con un porcentaje del cargo fijo mensual del servicio. El resultado del indicador de Disponibilidad se utiliza para establecer el factor de compensación.

Se valida en el Informe de Sanciones del primer semestre de 2014, sobre sanciones impuestas por la Superintendencia de Industria y Comercio en materia de Protección al Consumidor y Eficiencia de los Mercados, los siguientes Datos:

- Durante el primer semestre del año 2014 la Superintendencia de Industria y Comercio, impuso en primera instancia, 457 sanciones a empresas de diferentes sectores de la economía por contravención en las normas sobre protección al consumidor y eficiencia de los mercados, en donde el sector de telecomunicaciones está presente con un 11% y en materia de protección de datos personales un 1%, de sanciones generales, dicha relación se observa en la figura 5:

Figura 5. Sanciones Generales, Superintendencia de Industria y Comercio



Fuente: INFORME SANCIONES PRIMER SEMESTRE 2014, Sanciones impuestas por la Superintendencia de Industria y Comercio en materia de Protección al Consumidor y Eficiencia de los Mercados.

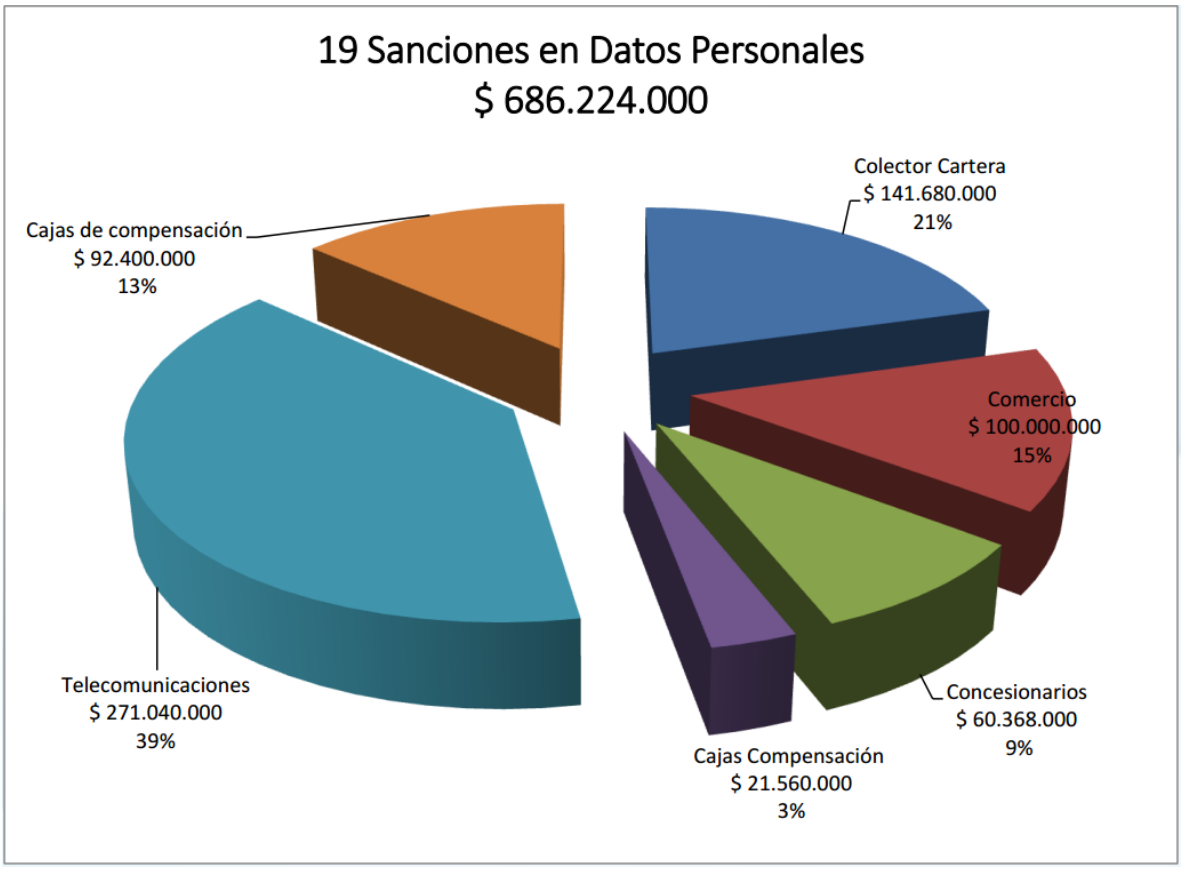
- La empresa de Telecomunicaciones para el tiempo del informe se encontraba en quinto lugar dentro de las seis empresas de servicios de telecomunicaciones más sancionadas como se muestra en la figura 6:

Figura 6. Empresas más sancionadas en servicios de comunicaciones

Fuente: INFORME SANCIONES PRIMER SEMESTRE 2014, Sanciones impuestas por la Superintendencia de Industria y Comercio en materia de Protección al Consumidor y Eficiencia de los Mercados.

- De las sanciones en materia de protección de datos personales para el primer semestre de 2014, el sector de telecomunicaciones obtuvo un 39% del total de las multas impuestas como se evidencia en la Figura 7:

Figura 7. Sanciones en datos personales



Fuente: INFORME SANCIONES PRIMER SEMESTRE 2014, Sanciones impuestas por la Superintendencia de Industria y Comercio en materia de Protección al Consumidor y Eficiencia de los Mercados.

Teniendo en cuenta la anterior información se realiza el análisis de contexto interno y externo del área de mesa de ayuda grandes clientes Empresa de Telecomunicaciones

En cuanto al ambiente externo se determinan los factores externos, las amenazas y situaciones de riesgo que pueden afectar el cumplimiento de los objetivos del

área durante la realización de labores en modalidad de Teletrabajo, teniendo esto en cuenta, la organización puede verse afectada en cuanto a factores económicos, legales y sociales como se observa en el cuadro 4:

Cuadro 4. Contexto Externo

CONTEXTO ESTRATÉGICO - ANÁLISIS EXTERNO		
Factores	**Amenazas**	**Situación de riesgo**
Económicos	• Descuentos en facturación de los clientes actuales por demora en solución de incidentes	• Malos tiempos de respuesta al cliente debido a problemas en la disponibilidad de los activos, problemas lentitud
	• Multas por incumplimiento de contrato	
Legales	• Violación de legislación aplicable, se faltaría a cláusulas de confidencialidad para manejo de información crítica de otras empresas	• Revelación de información crítica de la Empresa de Telecomunicaciones o de clientes por falla en manejo de información confidencial
Sociales	• Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos	• Información confusa o errónea al cliente debido a falta de integridad de la información que se maneja y problemas en la disponibilidad de elementos para la comunicación

Fuente: Autores

Se observa en el análisis externo del contexto, los factores, las amenazas y situaciones de riesgos encontradas para teletrabajo se asemejan a las presentadas en trabajo en sitio ya que para le empresa se debe apuntar a los mismos objetivos, el cambio a considerar es el nivel de exposición al riesgo que la realización en modalidad de Teletrabajo implica.

En el Cuadro 5 se menciona todo aquello dentro de la organización de la Mesa de Ayuda Grandes clientes de la Empresa de Telecomunicaciones que pueda tener influencia en la forma en que se gestiona el riesgo en el contexto de los objetivos de la información, allí se observan las capacidades de la organización, las debilidades y las situaciones de riesgo que amenazan el cumplimiento de los objetivos:

Cuadro 5. Contexto Interno

CONTEXTO ESTRATÉGICO - ANÁLISIS INTERNO		
Capacidad	**Debilidades**	**Situación de riesgo**
Administrativa	• Falta de seguimiento a las actividades realizadas por parte del teletrabajador, control y supervisión de las labores realizadas	Para las áreas directivas se podrían presentar dificultades en el seguimiento a los teletrabajadores
Operativa	• Falta de procedimientos operativos definidos para Teletrabajo en caso de contingencia	En caso de falla, la gestión incorrecta o nula de reportes, o la falta de información en la entrega turno, o en el escalamiento a otras áreas que podrían causar confusión y repercutir en el nivel de atención a los clientes
	• Incumplimiento de labores asignadas debido a problemas en la disponibilidad de los activos	El teletrabajador puede verse afectado por problemas en la conexión o en los equipos que utiliza para desempeñar su labor durante la jornada laboral
	• Falta de requerimientos y lineamientos de seguridad, que garanticen la disponibilidad, integridad y confidencialidad de la información en Teletrabajo	El teletrabajador puede cometer faltas a la seguridad de la información que afecten la disponibilidad, confidencialidad e integridad de la misma
	• Comunicación deficiente con áreas especializadas	Falta de integridad de la información que se maneja, problemas en la disponibilidad de elementos para la comunicación
Talento humano	• Falta de un plan de capacitación del personal en seguridad en el momento de realizar Teletrabajo	El teletrabajador puede cometer faltas a la seguridad de la información que afecten la disponibilidad, confidencialidad e integridad de la misma

Fuente: Autores

Se deben también puntualizar los activos de información que se encuentran comprometidos con el alcance de las labores por orientar al Teletrabajo, y su impacto y/o repercusión en los objetivos generales, antes mencionados, la cual se advierte en el siguiente cuadro:

Cuadro 6. Activos de información

		OBJETIVOS		
	Si Falla / Impacto	**Información Empresa**	**Información Clientes**	**Niveles de Servicio**
ACTIVOS	Teletrabajador	x	x	X
	Instalaciones			X
	Equipos de trabajo	x	x	X
	Conexión a Internet			X
	Acceso remoto a la red corporativa	x	x	X
	Aplicativo para registro y seguimiento de reportes	x	x	X
	Correo			X
	Base de datos de clientes		x	X
	Contacto telefónico			X

Fuente: Fuente: Empresa de Telecomunicaciones, adaptación del autor

El Cuadro 6 guarda relación con la identificación de los activos de información mencionados en el ítem 6.4 que indica las herramientas requeridas para la realización de Teletrabajo, y su pertinencia está justificada por la presencia de estas variables en el proceso de mesa de ayuda orientado al teletrabajo. Las variables consideradas en la primera columna se enlistan y se supeditan a una condición hipotética de falla o mala operación, y dada su naturaleza de activos de información, se mencionan los efectos y/o repercusiones que tendrían sobre la información de la Empresa de Telecomunicaciones, de los clientes, y en los niveles de servicio de la mesa de ayuda.

Alcance y límites de la gestión de riesgos

En esta fase se estableció los límites y alcance de la gestión de riesgos de seguridad de la información, en el contexto de la Empresa de Telecomunicaciones, a saber:

- La propuesta de seguridad para teletrabajo solo aplica a los ingenieros de la mesa de ayuda encargados de servicios cuya atención en 7x24, es decir 30 ingenieros de soporte de la mesa de ayuda.
- La mesa de ayuda ha realizado algunas pruebas piloto con 4 ingenieros del área que manejan clientes especiales, sin embargo, debido a que no están definidas y establecidas las políticas de seguridad para la conexión remota y el manejo seguro de la información en el área de Mesa de Ayuda, no se ha institucionalizado el modelo de teletrabajo como forma de trabajo para todos los ingenieros del área.
- La Empresa de Telecomunicaciones dispone de un conjunto de herramientas propicias para realizar Teletrabajo, y en tal sentido, se orienta la propuesta de seguridad sobre la base de las mismas.
- Esta propuesta de seguridad se enfoca a la conexión y elementos necesarios para Teletrabajo que están fuera de la red corporativa de la Empresa de Telecomunicaciones y por lo tanto fuera del alcance o sin gestión por parte de la empresa, ya que el manejo de la red corporativa, y las conexiones remotas que maneja, en este caso VPNs son administradas, gestionadas y salvaguardadas por el área de TI y Seguridad de la Empresa de Telecomunicaciones

Criterios del Riesgo

Se deben definir los criterios que se van a utilizar para evaluar la importancia del riesgo. Estos criterios deben reflejar los valores objetivos y recursos de la organización

Se tienen en cuenta los objetivos de seguridad más comunes aplicados a teletrabajo y acceso remoto según la Guía para Teletrabajo y seguridad en el acceso remoto de la NIST [*Guide to Enterprise Telework and Remote Access Security, NIST Special Publication 800-46 Revision 1, June 2009]*:

- La confidencialidad consiste en garantizar que las comunicaciones de acceso remoto y los datos de usuario almacenados no puedan ser leídos por personas no autorizadas
- Integridad que radica en detectar cualquier cambio intencional o no intencional a las comunicaciones de acceso remoto que se producen durante el transporte de la información
- Disponibilidad para garantizar que los usuarios puedan acceder a los recursos a través de acceso remoto cuando sea necesario.

Los criterios son desarrollados para la evaluación de los riesgos de seguridad de la información, y tienen en cuenta el valor estratégico de la información, estos criterios permiten establecer el orden en que deben ser tratados los riesgos identificados. En el cuadro 7, se determina junto con las directivas del área el nivel de aceptación de riesgo:

Cuadro 7. Criterios para la evaluación de riesgos

Objetivo	Mejorar tiempos de respuesta a requerimientos y reportes			
Riesgos	**Causas**	**Posibles Amenazas**	**Efectos**	**Aceptación**
Problemas en la disponibilidad de los activos, problemas lentitud	• Tele trabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	• La persona no se encuentra disponible para el proceso. • Fuente de alimentación no fiable • La ausencia de una conexión a Internet • Tecnologías incompatibles para el acceso a Internet • Pérdida o robo de equipos de teletrabajo • El daño a las computadoras de teletrabajo • Equipo teletrabajo no es adecuado para el teletrabajo • Acceso a Internet, mal funcionamiento del dispositivo • Mal funcionamiento de software de comunicaciones • Conexión a Internet no disponible • Conexión a Internet no fiable o lento • Acceso remoto a la red corporativa de la empresa no disponible continuamente	• Incumplimiento en los tiempos de respuesta acordados con el cliente lo que genera descuentos en facturación • Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos Media (3)	Grave

Cuadro 7. (Continuación)

Objetivo	Brindar información clara y confiable al cliente de los seguimientos y actividades realizadas para dar respuesta o solución al requerimiento			
Riesgos	**Causas**	**Posibles Amenazas**	**Efectos**	**Aceptación**
Falta de integridad de la información que se maneja, problemas en la disponibilidad de elementos para la comunicación	• Tele trabajador • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	• La elección de contraseñas débiles • Introducción de malware a través de Internet o correo electrónico • La introducción de malware de soportes de datos portátiles • Negligencia de importantes actividades 'limpieza' • La carga de software dañino • Cambios inapropiados en la configuración del software • Protección contra malware inadecuada	• Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos Baja (2)	Manejable

Cuadro 7. (Continuación)

Objetivo	Documentar todas las actividades realizadas en el reporte			
Riesgos	**Causas**	**Posibles Amenazas**	**Efectos**	**Aceptación**
Problemas en la disponibilidad de los activos	• Tele trabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	• La persona no se encuentra disponible para el proceso. • Fuente de alimentación no fiable • La ausencia de una conexión a Internet • Tecnologías incompatibles para el acceso a Internet • Pérdida o robo de equipos de teletrabajo • El daño a las computadoras de teletrabajo • Equipo teletrabajo no es adecuado para el teletrabajo • Acceso a Internet, mal funcionamiento del dispositivo • Mal funcionamiento de software de comunicaciones • Conexión a Internet no disponible • Conexión a Internet no fiable o lento • Acceso remoto a la red corporativa de la empresa no disponible continuamente	• En caso de solicitud de informes por parte de los clientes, o entes de control del manejo y actividades realizadas en los reportes no se contaría con sustento • No se tiene un seguimiento a las actividades realizadas por parte del teletrabajador, se pierde el control y supervisión de las labores realizadas Baja (2)	Manejable

Cuadro 7. (Continuación)

Objetivo	Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma			
Riesgos	**Causas**	**Posibles Amenazas**	**Efectos**	**Aceptación**
Falla en manejo de información confidencial	• Tele trabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	• La divulgación de la información de inicio de sesión • La elección de contraseñas débiles • Conexión del equipo teletrabajo a las redes informáticas pública • Equipos de teletrabajo en daño en manos de terceros • El uso de los ordenadores de teletrabajo por parte de terceros • Inspección de la información a través de vistas • Control de acceso lógico en el ordenador teletrabajo anulada • Las características de seguridad no configurados correctamente • Descubrimiento de información de inicio de sesión que se almacena en el ordenador del teletrabajo • Las claves de cifrado almacenadas en el ordenador teletrabajo comprometidas • La inspección no autorizada de datos en tránsito • Secuestro de la conexión • Conexiones no utilizadas permanecen abiertas • Teletrabajador tiene demasiados derechos de acceso a la red corporativa de la empresa de forma remota • Personas no autorizadas tengan acceso remoto a la red corporativa	• Violación de legislación aplicable, se faltaría a cláusulas de confidencialidad para manejo de información crítica de otras empresas (verificar implicación legal) • Posibles intrusiones tanto a la red de la Empresa de Telecomunicaciones como a la de sus clientes específicos que puede resultar en afectación de servicios, robo o cambio de información, con implicaciones legales, económicas y de reputación de la organización Alta (4)	Inaceptable

Cuadro 7. (Continuación)

Objetivo	Cumplir oportunamente con labores asignadas			
Riesgos	**Causas**	**Posibles Amenazas**	**Efectos**	**Aceptación**
Problemas en la disponibilidad de los activos	• Tele trabajador • Instalaciones • Equipo de trabajo • Conexión a Internet	La persona no se encuentra disponible para el proceso. Fuente de alimentación no fiable La ausencia de una conexión a Internet Tecnologías incompatibles para el acceso a Internet Pérdida o robo de equipos de teletrabajo El daño a las computadoras de teletrabajo Equipo teletrabajo no es adecuado para el teletrabajo Acceso a Internet, mal funcionamiento del dispositivo Mal funcionamiento de software de comunicaciones Conexión a Internet no disponible Conexión a Internet no fiable o lento Acceso remoto a la red corporativa de la empresa no disponible continuamente	• Incumplimiento en los tiempos de respuesta acordados con el cliente lo que genera descuentos en facturación • Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos Media (3)	Grave

Cuadro 7. (Continuación)

Objetivo	Mantener una comunicación e interacción eficaz con otras áreas especializadas			
Riesgos	**Causas**	**Posibles Amenazas**	**Efectos**	**Aceptación**
Falta de integridad de la información que se maneja, problemas en la disponibilidad de elementos para la comunicación	• Tele trabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Contacto telefónico	• La elección de contraseñas débiles • Introducción de malware a través de Internet o correo electrónico • La introducción de malware de soportes de datos portátiles • Negligencia de importantes actividades 'limpieza' • La carga de software dañino • Cambios inapropiados en la configuración del software • Protección contra malware inadecuada	• Incumplimiento en los tiempos de respuesta acordados con el cliente lo que genera descuentos en facturación • Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos Media (3)	Grave

Fuente: Autores

Cuadro 8. Niveles de aceptación de riesgos

Nivel de medición	Nivel de aceptación
Alta (4)	Inaceptable
Media (3)	Grave
Baja (2)	Manejable

Fuente: Autores

En el cuadro anterior, basados en los objetivos específicos definidos por la empresa, los riesgos generales, los activos en juego para dar cumplimiento a cada objetivo, las amenazas presentadas y los posibles efectos de incumplimiento de dichos objetivos, se determina por parte de la Mesa de Ayuda los niveles de aceptación de riesgos.

De este ejercicio, se evidenció el riesgo que presenta mayor prioridad o es inaceptable para la empresa, lo constituye la falla en el manejo de información confidencial tanto de la Empresa de Telecomunicaciones como de sus clientes.

7.2 VALORACIÓN DEL RIESGO

En esta etapa se procedió con la total de identificación del riesgo, su análisis, y su evaluación.

- **Identificación de riesgo**

En este punto es necesario identificar las fuentes de riesgo, las áreas de impacto, los eventos, sus causas y consecuencias potenciales. Se debe generar un listado de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos

Se realiza un cuadro con la definición de procesos, actividades, objetivos y su relación con los activos involucrados en el proceso, en donde se encuentran los activos con más utilización dentro de las actividades realizadas

Cuadro 9. Identificación de activos

Proceso	Actividad	Objetivo	Activos involucrados en el proceso
Registro turno	Inicio de Turno	• Cumplir del horario laboral, registro puntual del inicio de labores • Mejorar tiempos de respuesta a requerimientos y reportes	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Acceso remoto a red corporativa
Seguimiento	Recepción de reportes para seguimiento	•Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Correo electrónico
Reporte de Cliente	Recepción de nuevos reportes	•Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Aplicativo para registro y seguimiento de reportes
Pruebas Iniciales	Búsqueda de información de cliente y servicio reportado	•Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Mejorar tiempos de respuesta a requerimientos y reportes	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Acceso remoto a red corporativa 6. Base de datos clientes

Cuadro 9. (Continuación)

Proceso	Actividad	Objetivo	Activos involucrados en el proceso
Pruebas Iniciales	Pruebas de primer nivel	• Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Mejorar tiempos de respuesta a requerimientos y reportes	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Acceso remoto a red corporativa
Seguimiento	Seguimiento a reportes en herramienta de gestión	• Manejar información confidencial de cada cliente de forma responsable • Manejar información confidencial de la Empresa de Telecomunicaciones de forma responsable • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Aplicativo para registro y seguimiento de reportes
Seguimiento	Avances al cliente mediante correo	• Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Correo electrónico
Seguimiento	Avances telefónicos al cliente	• Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Contacto telefónico

Cuadro 9. (Continuación)

Proceso	Actividad	Objetivo	Activos involucrados en el proceso
Escalamiento del reporte	Escalamiento a otras áreas mediante correo	• Comunicación e interacción eficaz con otras áreas especializadas	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Correo electrónico
Escalamiento del reporte	Escalamiento telefónico a otras áreas	• Comunicación e interacción eficaz con otras áreas especializadas	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Contacto telefónico
Seguimiento	Confirmación de operatividad con el cliente vía correo	• Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Contacto telefónico
Seguimiento	Confirmación de operatividad con el cliente telefónica	• Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Contacto telefónico

Cuadro 9. (Continuación)

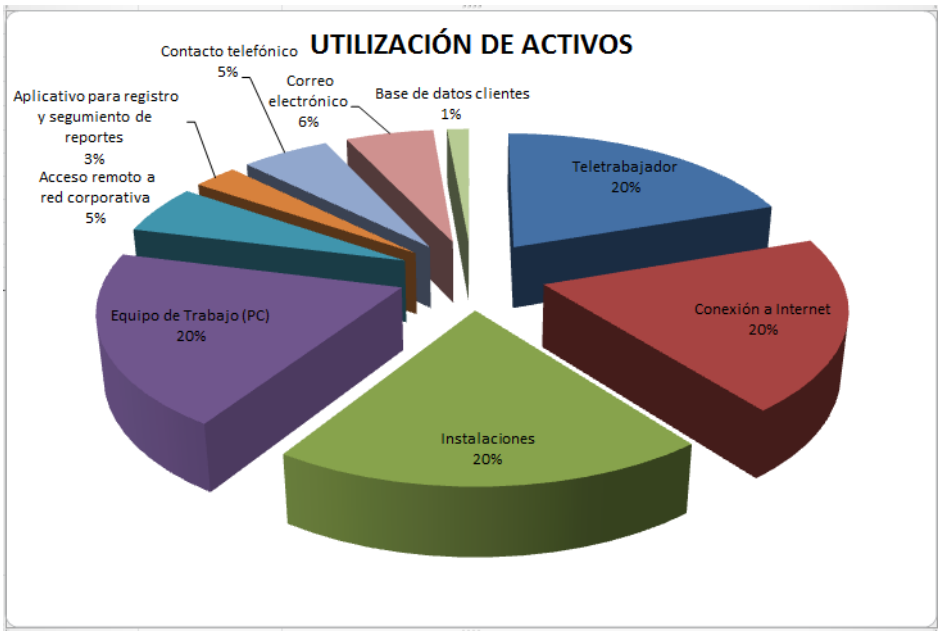
Proceso	Actividad	Objetivo	Activos involucrados en el proceso
Seguimiento	Envío de reportes para seguimiento	• Proteger la información confidencial de la Empresa de Telecomunicaciones y de cada cliente, a través de un manejo de forma responsable de la misma • Brindar información clara y confiable al cliente de los seguimientos o actividades realizadas para dar respuesta o solución al requerimiento • Documentar todas las actividades realizadas en el reporte	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Correo electrónico
Registro turno	Finalización de Turno	• Cumplimiento del horario laboral, registro puntual del finalización de labores • Mejorar tiempos de respuesta a requerimientos y reportes	1. Teletrabajador 2. Conexión a Internet 3. Instalaciones 4. Equipo de Trabajo (PC) 5. Acceso remoto a red corporativa

Fuente: Autores

Resultado de la realización de esta actividad, se obtuvo que los activos con mayor utilización durante los procesos y actividades correspondientes, son:

- El Teletrabajador
- Conexión a Internet
- Instalaciones
- Equipo de trabajo

Figura 8. Utilización de activos



Fuente: Autores

- **Análisis de Riesgo**

El análisis implica el desarrollo y la comprensión del riesgo; brinda una entrada para la toma de decisiones en la cual se deben hacer elecciones y las opciones implican diversos tipos y niveles de riesgo

El análisis de riesgos involucra la consideración de las causas y las fuentes de riesgo, sus consecuencias, y la probabilidad de ocurrencia, entre otros atributos del riesgo.

En este paso, se definen para los diferentes tipos de activos presentes en teletrabajo, el impacto de la fallas en cada a uno en cuanto a las características de la seguridad en la información. Se agrupan los activos de información de la siguiente manera:

Personas: Teletrabajador
Hardware: Equipos de trabajo, Teléfono móvil, Instalaciones

Servicios: Conexión a Internet, Correo, Acceso a la red corporativa
Información: Base de Datos de Clientes
Software: Aplicativo para registro y reportes

Se validan los riesgos a la disponibilidad, integridad y confidencialidad de la información para cada grupo:

Cuadro 10. Clasificación de riesgos por impacto

Activo / Característica	Confidencialidad	Integridad	Disponibilidad
Teletrabajador (Persona)	Se hace uso inadecuado de la información privilegiada a la cual se tiene acceso por cargo o función que desempeña. Media (3)	La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempeñar el rol o función. Baja (2)	La persona no se encuentra disponible para el proceso. Alta (4)
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Alguien conoce que existe el elemento o su configuración o accede al activo sin autorización. Alta (4)	El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente. Ejemplo: cuando se daña un elemento o parte del activo o funciona inadecuadamente. Media (3)	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado. Alta (4)
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Alguien conoce su existencia o configuración o hace uso no autorizado del activo. Media (3)	Se pierde la completitud, exactitud o precisión del servicio. Debido a que el servicio no se presta en las condiciones óptimas y acordadas. Media (3)	El activo no está disponible o no se puede tener acceso a él cuando se requiere y por el personal que está autorizado Alta (4)
Bases de datos de clientes (Información)	Individuo, entidad o proceso no autorizado accede al activo de información. Alta (4)	Se pierde la completitud, exactitud o precisión del activo de información. Ejemplo: Errores de procesamiento de los sistemas. Baja (2)	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado Media (3)
Aplicativo para registro y reportes (Software)	Individuo, entidad o proceso no autorizado conoce la existencia o parametrización del activo Baja (2)	Se valora la completitud, exactitud o precisión de la parametrización del activo. Ejemplo: modificación la configuración del software lo que puede llevar a errores en la información a procesar Baja (2)	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado Alta (4)

Fuente: Autores

Cuadro 11. Descripción de Niveles de Impacto

Nivel	Descripción de Impacto en Confidencialidad	Descripción de Impacto en Integridad	Descripción de Impacto en Disponibilidad
Alto (4)	El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente a la empresa	Información cuya modificación no autorizada, no podría repararse, impidiendo la realización de actividades	Debe estar disponible el 99% del tiempo
Medio (3)	El conocimiento o divulga**c**ión no autorizada de la información que gestiona este activo impacta negativamente no sólo el proceso evaluado sino otros procesos, serían relevantes, el incidente implicaría otras áreas	Información cuya modificación no autorizada, es de difícil reparación y podría ocasionar un perjuicio significativo	Debe estar disponible el 50% del tiempo
Bajo (2)	El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente de manera leve al proceso. Daños bajos, el incidente no trascendería del área afectada	Información cuya modificación no autorizada puede repararse aunque podría ocasionar un perjuicio	Debe estar disponible el 10% del tiempo
Muy Bajo (1)	El conocimiento o divulgación no autorizada de la información que gestiona este activo no impacta negativamente al proceso.	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta las actividades	Información cuya inaccesibilidad no afecta la actividad normal

Fuente: Autores

Cuadro 12. Resultado clasificación de riesgos por impacto

Activo / Característica	Confidencialidad	Integridad	Disponibilidad	Criticidad
Teletrabajador (Persona)	Medio (3)	Bajo (2)	Alto (4)	**MEDIO**
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Alto (4)	Medio (3)	Alto (4)	**ALTO**
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Medio (3)	Medio (3)	Alto (4)	**MEDIO**
Bases de datos de clientes (Información)	Alto (4)	Bajo (2)	Medio (3)	**MEDIO**
Aplicativo para registro y reportes (Software)	Bajo (2)	Bajo (2)	Alto (4)	**BAJO**

Fuente: Autores

Posteriormente se determinó que los eventos con criticidad alta se encuentran relacionados con los activos en el grupo hardware, como son el equipo de trabajo, las instalaciones y el teléfono móvil.

De igual manera, se determinó la probabilidad de ocurrencia de dichas fallas, obteniendo los siguientes resultados:

Cuadro 13. Clasificación de riesgos por probabilidad

Activo / Característica	Confidencialidad	Integridad	Disponibilidad
Teletrabajador (Persona)	Se hace uso inadecuado de la información privilegiada a la cual se tiene acceso por cargo o función que desempeña. Baja (2)	La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempeñar el rol o función. Baja (2)	La persona no se encuentra disponible para el proceso. Media (3)
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Alguien conoce que existe el elemento o su configuración o accede al activo sin autorización. Media (3)	El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente. Ejemplo: cuando se daña un elemento o parte del activo o funciona inadecuadamente. Media (3)	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado. Alta (4)
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Alguien conoce su existencia o configuración o hace uso no autorizado del activo. Media (3)	Se pierde la completitud, exactitud o precisión del servicio. Debido a que el servicio no se presta en las condiciones óptimas y acordadas. Baja (2)	El activo no está disponible o no se puede tener acceso a él cuando se requiere y por el personal que está autorizado Alta (4)
Bases de datos de clientes (Información)	Individuo, entidad o proceso no autorizado accede al activo de información. Baja (2)	Se pierde la completitud, exactitud o precisión del activo de información. Ejemplo: Errores de procesamiento de los sistemas. Muy Baja (1)	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado Baja (2)
Aplicativo para registro y reportes (Software)	Individuo, entidad o proceso no autorizado conoce la existencia o parametrización del activo Baja (2)	Se valora la completitud, exactitud o precisión de la parametrización del activo. Ejemplo: modificación la configuración del software lo que puede llevar a errores en la información a procesar Media (3)	El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado Alta (4)

Fuente: Autores

Cuadro 14. Descripción de niveles de probabilidad

Nivel	Descriptor	Descripción	Frecuencia
Alto	**Casi Seguro (4)**	Se espera que el evento ocurra en la mayoría de circunstancias	Más de 3 vez al año
Medio	**Probable (3)**	El evento probablemente ocurrirá en la mayoría de circunstancias	Más de 1 vez al año
Bajo	**Posible (2)**	El evento podría ocurrir en algún momento	Al menos una vez en el último año
Muy Bajo	**Raro (1)**	El evento puede ocurrir solo en circunstancias excepcionales	Al menos 1 vez en los últimos 2 años

Fuente: Autores

Cuadro 15. Resultado de Clasificación de riesgos por probabilidad

Activo / Característica	Confidencialidad	Integridad	Disponibilidad	Probabilidad
Teletrabajador (Persona)	Posible (2)	Posible (2)	Probable (3)	**BAJO**
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Probable (3)	Probable (3)	Casi Seguro (4)	**MEDIO**
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Probable (3)	Posible (2)	Casi Seguro (4)	**ALTO**
Bases de datos de clientes (Información)	Posible (2)	Raro (1)	Posible (2)	**MUY BAJO**
Aplicativo para registro y reportes (Software)	Posible (2)	Probable (3)	Casi Seguro (4)	**MEDIO**

Fuente: Autores

Del desarrollo del anterior ejercicio, se observó que nivel de ocurrencia medio indica que el evento probablemente ocurrirá en la mayoría de las circunstancias. Esta situación opera para los eventos relacionados con los activos en el grupo de servicios, seguidos de los de ocurrencia media como son hardware y software.

Basado en la clasificación realizada, se realizó la Matriz de Calificación, evaluación y respuesta a los Riesgos con el fin de determinar la zona de riesgo en la que se ubica el Teletrabajo en la mesa de ayuda con respecto a características de confidencialidad integridad y disponibilidad.

Para este fin, dado los pesos asignados a cada riesgo según el impacto como se muestra en el Cuadro 16, se realiza la sumatoria de los mismos con respecto a las columnas correspondientes a las características de confidencialidad, integridad y disponibilidad para encontrar un nivel de impacto relacionado a cada característica; dicho resultado se encuentra en el cuadro 17

De este modo, se determinaron los niveles de impacto con respecto a las características de seguridad de la información a proteger; encontrando un impacto alto para los eventos de riesgo que afectan la disponibilidad y que desvían el proceso del objetivo a alcanzar, como lo es, el mantener los niveles de servicio con los clientes, seguido de los eventos de riesgo que afectan la confidencialidad y con más baja criticidad los que afectan la integridad de la información.

Cuadro 16. Niveles de impacto según características de seguridad en la información

Activo / Característica	Confidencialidad	Integridad	Disponibilidad
Teletrabajador (Persona)	Medio (3)	Bajo (2)	Alto (4)
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Alto (4)	Medio (3)	Alto (4)
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Medio (3)	Medio (3)	Alto (4)
Bases de datos de clientes (Información)	Alto (4)	Bajo (2)	Medio (3)
Aplicativo para registro y reportes (Software)	Bajo (2)	Bajo (2)	Alto (4)

Fuente: Autores

Cuadro 17. Resultado de impacto según características de seguridad en la información

Característica	Confidencialidad	Integridad	Disponibilidad
Resultado	**16**	**12**	**19**
Nivel de Impacto	**Medio (3)**	**Bajo (2)**	**Alto (4)**

Fuente: Autores

Teniendo en cuenta los pesos asignados a cada riesgo según su probabilidad como se muestra en el cuadro 18, se realiza igualmente sumatoria de tales valores con respecto a las columnas correspondientes a las características de confidencialidad, integridad y disponibilidad; y así encontrar el nivel de probabilidad respectivo a cada característica, este resultado se puede observar en el cuadro 19

Con respecto a la probabilidad de ocurrencia de los eventos de riesgo, se encontró en la mayoría de las circunstancias que existe mayor probabilidad de que sucedan los eventos de riesgo afectando la disponibilidad, seguido de los que afectan la confidencialidad e integridad con nivel bajo que indica que los eventos podrían ocurrir en algún momento.

Cuadro 18. Nivel de probabilidad según características de seguridad en la información

Activo / Característica	Confidencialidad	Integridad	Disponibilidad
Teletrabajador (Persona)	Posible (2)	Posible (2)	Probable (3)
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Probable (3)	Probable (3)	Casi Seguro (4)
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Probable (3)	Posible (2)	Casi Seguro (4)
Bases de datos de clientes (Información)	Posible (2)	Raro (1)	Posible (2)

Aplicativo para registro y reportes (Software)	Posible (2)	Probable (3)	Casi Seguro (4)

Fuente: Autores

Cuadro 19. Resultado de probabilidad según características de seguridad en la información

Característica	Confidencialidad	Integridad	Disponibilidad
Resultado	**12**	**11**	**17**
Nivel de Impacto	**Posible (2)**	**Posible (2)**	**Casi Seguro (4)**

Fuente: Autores

- **Matriz Resultado Riesgos**

Una vez acometidas las etapas anteriores, se determinó el nivel del riesgo de acuerdo a la Matriz de calificación y determinación del Nivel de Riesgo:

Inicialmente se determina la matriz de clasificación en la cual se basa este ejercicio, para ello se determinan los valores que indicarán las zonas de riesgo se muestra en los cuadros 20 y 21 a continuación

Cuadro 20. Matriz de calificación

	Impacto			
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**
Raro (1)	1	2	3	4
Posible (2)	2	4	6	8
Probable (3)	3	6	9	12
Casi Seguro (4)	4	8	12	16

Fuente: CENS, adaptación del autor

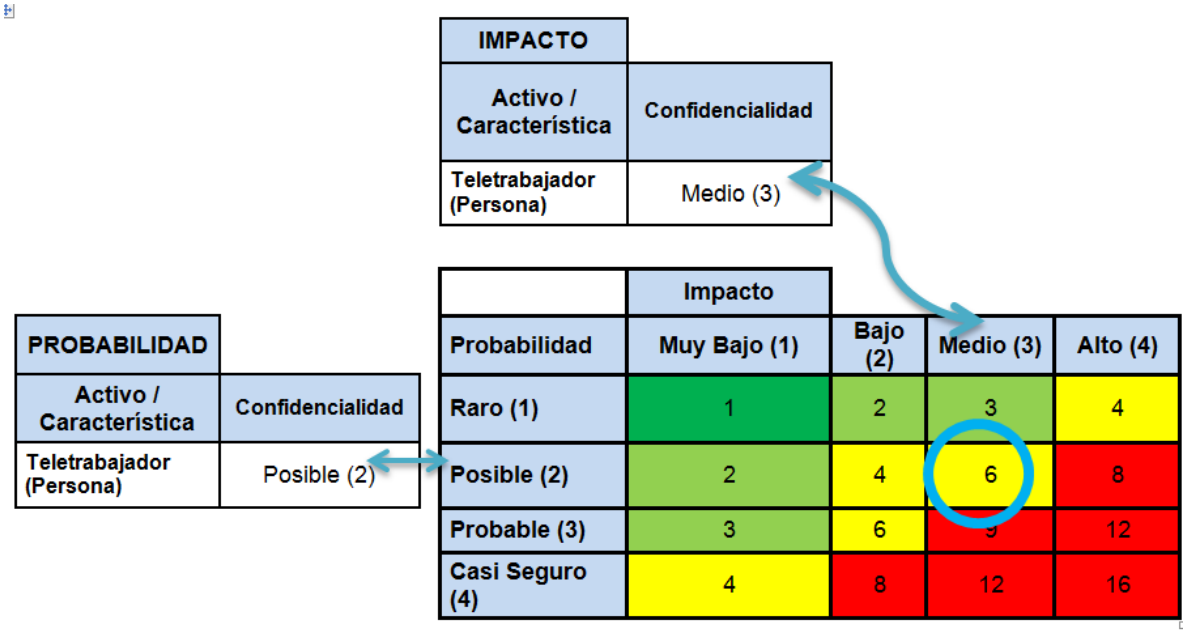
Cuadro 21. Acción según Zona de Riesgo

Zona	Acción	Valor
Zona de Riesgo Muy Baja	Asumir el riesgo	1
Zona de Riesgo Baja	Asumir el Riesgo, Reducir el Riesgo	2 a 3
Zona de Riesgo Media	Reducir el Riesgo, Evitar, Compartir o transferir	4 a 6
Zona de Riesgo Alta	Reducir el Riesgo, Evitar, Compartir o transferir	7 a 16

Fuente: Autores

Paso a seguir, se calcula la zona de riesgo, para el estudio de interés del presente proyecto, basado en los cuadros 16 y 18, clasificando los riesgos según la matriz expuesta en el cuadro 20, así:
Se verifican los niveles determinados para el riesgo en las tablas de impacto y probabilidad en los cuadros 16 y 18 respectivamente, se realiza la ubicación de los niveles correspondientes el cuadro 20, y según su ubicación se indica la zona de riesgo como resultado en el cuadro 22

Figura 9. Cálculo de Zona de Riesgo



Fuente: Autores

Cuadro 22. Determinación del Nivel de Riesgo

Activo / Característica	Confidencialidad	Integridad	Disponibilidad
Teletrabajador (Persona)	Zona de Riesgo Media (3)	Zona de Riesgo Media (3)	Zona de Riesgo Alta (4)
Equipos de trabajo, teléfono, Instalaciones (Hardware)	Zona de Riesgo Alta (4)	Zona de Riesgo Alta (4)	Zona de Riesgo Alta (4)
Conexión a Internet, acceso a la red corporativa, correo (Servicio)	Zona de Riesgo Alta (4)	Zona de Riesgo Media (3)	Zona de Riesgo Alta (4)
Bases de datos de clientes (Información)	Zona de Riesgo Alta (4)	Zona de Riesgo Baja (2)	Zona de Riesgo Media (3)
Aplicativo para registro y reportes (Software)	Zona de Riesgo Media (3)	Zona de Riesgo Media (3)	Zona de Riesgo Alta (4)

Fuente: Autores

Se establece la zona de riesgo según las características de seguridad de la información registrada en el cuadro 23, realizando la sumatoria los valores de las columnas del cuadro 22:

Cuadro 23. Resultado Determinación del Nivel de Riesgo

Característica	Confidencialidad	Integridad	Disponibilidad
Resultado	**18**	**15**	**19**
Nivel de Impacto	**Zona de Riesgo Alta (4)**	**Zona de Riesgo Media (3)**	**Zona de Riesgo Alta (4)**

Fuente: Autores

Como resultados de la anterior aplicación, se encontró que los esfuerzos se deben dirigir en más alto grado hacia salvaguardar la disponibilidad y confidencialidad de los activos.

Valoración de Riesgo

El propósito de este punto es facilitar la toma de decisiones, basada en los resultados del análisis anterior, acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento

En el análisis realizado hasta el momento se determinan los siguientes aspectos, en donde se observan las principales características de la información y activos involucrados en el riesgo, a los cuales se debe priorizar en la concepción de controles:

Cuadro 24. Resumen de análisis de Riesgo Inicial

	Activo		Característica	
Criticidad	**Alta**	**Media**	**Alta**	**Media**
Aceptabilidad	NA	NA	Confidencialidad	Disponibilidad
Impacto	Hardware	Servicios	Disponibilidad	Confidencialidad
Probabilidad	Servicios	Hardware	Disponibilidad	Confidencialidad
Zona de Riesgo	Hardware	Servicios	Disponibilidad	Confidencialidad

Fuente: Autores

Se validan los siguientes riesgos generales:

Riesgo 1. Malos tiempos de respuesta al cliente debido a problemas en la disponibilidad de los activos, problemas lentitud.

Riesgo 2. Información confusa o errónea al cliente debido a falta de integridad de la información que se maneja y problemas en la disponibilidad de elementos para la comunicación.

Riesgo 3. Falta de documentación y seguimiento de actividades realizadas debido a problemas en la disponibilidad de los activos.

Riesgo 4. Revelación de información crítica de la Empresa de Telecomunicaciones o del cliente por falla en manejo de información confidencial.

Riesgo 5. Incumplimiento de labores asignadas debido a problemas en la disponibilidad de los activos.

Riesgo 6. Comunicación deficiente con áreas especializadas para solución de fallas o respuesta a requerimientos, debido a la falta de integridad de la información que se maneja, problemas en la disponibilidad de elementos para la comunicación.

Siguiendo con el abordaje metodológico sugerido desde la norma tomada como referencia, se procedió a la aplicación de la valoración de riesgo como se ve en los cuadros 25 al 30, a saber:

Cuadro 25. Valoración Riesgo 1

Riesgos	Causas	Característica	Efectos
Malos tiempos de respuesta al cliente debido a problemas en la disponibilidad de los activos, problemas lentitud	• Teletrabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	**Disponibilidad** • La persona no se encuentra disponible para el proceso. • El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado. • El activo no está disponible o no se puede tener acceso a él cuando se requiere y por el personal que está autorizado	• Incumplimiento en los tiempos de respuesta acordados con el cliente lo que genera descuentos en facturación • Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos

	Impacto				Prioridad
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	
Raro (1)					Alta
Posible (2)					
Probable (3)					
Casi Seguro (4)				X	

Fuente: Autores

Cuadro 26. Valoración Riesgo 2

Riesgos	Causas	Característica	Efectos
Información confusa o errónea al cliente debido a falta de integridad de la información que se maneja y problemas en la disponibilidad de elementos para la comunicación	• Tele trabajador • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	**Integridad** • La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempeñar el rol o función. • El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente. Ejemplo: cuando se daña un elemento o parte del activo o funciona inadecuadamente. • Se pierde la completitud, exactitud o precisión del servicio. Debido a que el servicio no se presta en las condiciones óptimas y acordadas. • Se pierde la completitud, exactitud o precisión del activo de información. Ejemplo: Errores de procesamiento de los sistemas. • Se valora la completitud, exactitud o precisión de la parametrización del activo. Ejemplo: modificación la configuración del software lo que puede llevar a errores en la información a procesar	• Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos

	Impacto				Prioridad
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	
Raro (1)					Media
Posible (2)		X			
Probable (3)					
Casi Seguro (4)					

Fuente: Autores

Cuadro 27. Valoración Riesgo 3

Riesgos	Causas	Característica	Efectos
Falta de documentación y seguimiento de actividades realizadas debido a problemas en la disponibilidad de los activos	• Tele trabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Base de datos clientes • Contacto telefónico	**Disponibilidad** • La persona no se encuentra disponible para el proceso. • El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado. • El activo no está disponible o no se puede tener acceso a él cuando se requiere y por el personal que está autorizado	En caso de solicitud de informes por parte de los clientes, o entes de control del manejo y actividades realizadas en los reportes no se contaría con sustento No se tiene un seguimiento a las actividades realizadas por parte del teletrabajador, se pierde el control y supervisión de las labores realizadas

	Impacto				Prioridad
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	
Raro (1)					Alta
Posible (2)					
Probable (3)					
Casi Seguro (4)				X	

Fuente: Autores

Cuadro 28. Valoración Riesgo 4

Riesgos	Causas	Característica	Efectos
Revelación de información crítica de la Empresa de Telecomunicaciones o del cliente por falla en manejo de información confidencial	Tele trabajador Instalaciones Equipo de trabajo Acceso remoto a red corporativa Conexión a Internet Aplicativo para registro y seguimiento de reportes Correo Base de datos clientes Contacto telefónico	**Confidencialidad** • Se hace uso inadecuado de la información privilegiada a la cual se tiene acceso por cargo o función que desempeña. • Alguien conoce que existe el elemento o su configuración o accede al activo sin autorización. • Alguien conoce su existencia o configuración o hace uso no autorizado del activo. • Individuo, entidad o proceso no autorizado accede al activo de información. • Individuo, entidad o proceso no autorizado conoce la existencia o parametrización del activo	Violación de legislación aplicable, se faltaría a cláusulas de confidencialidad para manejo de información crítica de otras empresas (verificar implicación legal) Posibles intrusiones tanto a la red de la Empresa de Telecomunicaciones como a la de sus clientes específicos que puede resultar en afectación de servicios, robo o cambio de información, con implicaciones legales, económicas y de reputación de la organización

	Impacto				Prioridad
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	
Raro (1)					Media
Posible (2)			X		
Probable (3)					
Casi Seguro (4)					

Fuente: Autores

Cuadro 29. Valoración Riesgo 5

Riesgos	Causas	Característica	Efectos
Incumplimiento de labores asignadas debido a problemas en la disponibilidad de los activos	• Tele trabajador • Instalaciones • Equipo de trabajo • Conexión a Internet	**Disponibilidad** • La persona no se encuentra disponible para el proceso. • El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado. • El activo no está disponible o no se puede tener acceso a él cuando se requiere y por el personal que está autorizado • El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado • El activo de información no puede ser accedido o utilizado cuando se requiere y por el personal que está autorizado	• Incumplimiento en los tiempos de respuesta acordados con el cliente lo que genera descuentos en facturación • Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos

	Impacto				Prioridad
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	
Raro (1)					Alta
Posible (2)					
Probable (3)					
Casi Seguro (4)				X	

Fuente: Autores

Cuadro 30. Valoración Riesgo 6

Riesgos	Causas	Característica	Efectos
Comunicación deficiente con áreas especializadas para solución de fallas o respuesta a requerimientos, debido a la falta de integridad de la información que se maneja, problemas en la disponibilidad de elementos para la comunicación	• Tele trabajador • Instalaciones • Equipo de trabajo • Acceso remoto a red corporativa • Conexión a Internet • Aplicativo para registro y seguimiento de reportes • Correo • Contacto telefónico	**Integridad** • La persona produce datos errados o incompletos o de acuerdo con su rol toma decisiones equivocadas, por capacidades o aptitudes inadecuadas para desempeñar el rol o función. • El activo no efectúa las actividades de procesamiento o su función correctamente o es alterada su configuración indebidamente. Ejemplo: cuando se daña un elemento o parte del activo o funciona inadecuadamente. • Se pierde la completitud, exactitud o precisión del servicio. Debido a que el servicio no se presta en las condiciones óptimas y acordadas. • Se pierde la completitud, exactitud o precisión del activo de información. Ejemplo: Errores de procesamiento de los sistemas. • Se valora la completitud, exactitud o precisión de la parametrización del activo. Ejemplo: modificación la configuración del software lo que puede llevar a errores en la información a procesar	• Incumplimiento en los tiempos de respuesta acordados con el cliente lo que genera descuentos en facturación • Quejas por parte de los clientes, que en su medida afectan la reputación de la misma teniendo esto impacto en la ventas y renovación de contratos

	Impacto				Prioridad
Probabilidad	**Muy Bajo (1)**	**Bajo (2)**	**Medio (3)**	**Alto (4)**	
Raro (1)					Media
Posible (2)		X			
Probable (3)					
Casi Seguro (4)					

Fuente: Autores

Tomando como base el anterior ejercicio se realizó un listado de amenazas, con su correspondiente análisis de repercusión en las características de seguridad de la información, el cual se puede advertir en el cuadro 31:

Cuadro 31. Identificación de amenazas

Activo	Amenaza	Confidencialidad	Integridad	Disponibilidad
El teletrabajador	El Ingeniero no se encuentra disponible para el proceso.			x
	La divulgación de la información de inicio de sesión	x		
	La elección de contraseñas débiles	x	x	
	Introducción de malware a través de Internet o correo electrónico		x	
	La introducción de malware de soportes de datos portátiles		x	
	Conexión del equipo teletrabajo a las redes públicas	x		
	Equipos de teletrabajo en daño en manos de terceros	x		
	El uso de los ordenadores de teletrabajo por parte de terceros	x		
	Negligencia de importantes actividades de mantenimiento		x	
	La carga de software dañino		x	
	Cambios inapropiados en la configuración del software		x	
Instalaciones	Fuente de alimentación no fiable			x
	La ausencia de una conexión a Internet			x
	Tecnologías incompatibles para el acceso a Internet			x
	Pérdida o robo de equipos de teletrabajo			x
	El daño a las computadoras de teletrabajo			x
	Inspección de la información a través de vistas	x		

Cuadro 31. (Continuación)

Activo	Amenaza	Confidencialidad	Integridad	Disponibilidad
El equipo teletrabajo	Equipo teletrabajo no es adecuado para el teletrabajo			x
	Control de acceso lógico anulado en el ordenador de teletrabajo	x		
	Las características de seguridad no configurados correctamente	x		
	Protección contra malware inadecuada		x	
	Descubrimiento de información de inicio de sesión que se almacena en el ordenador del teletrabajo	x		
	Las claves de cifrado almacenadas en el ordenador teletrabajo comprometidas	x		
	Acceso a Internet, mal funcionamiento del dispositivo			x
	Mal funcionamiento de software de comunicaciones			x
La conexión a Internet	Conexión a Internet no disponible			x
	Conexión a Internet no fiable o lento			x
	La inspección no autorizada de datos en tránsito	x		
	Secuestro de la conexión	x	x	
	Conexiones no utilizadas permanecen abiertas	x	x	
Acceso remoto a la red corporativa de la empresa	Acceso remoto a la red corporativa de la empresa no disponible continuamente			x
	Teletrabajador tiene demasiados derechos de acceso a la red corporativa de la empresa de forma remota	x		
	Personas no autorizadas tengan acceso remoto a la red corporativa	x		

Fuente: Autores

7.3 TRATAMIENTO DE RIESGO

El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica

Controles existentes en la Empresa de Telecomunicaciones que aplican a Teletrabajo

Antes de abordar lo concerniente a los controles y salvaguardas a los activos se hizo necesario examinar los controles existentes en la Empresa de Telecomunicaciones que podrían ser aplicados al teletrabajo. Como resultado de dicho ejercicio se identificaron dos niveles de requisitos: los primeros de naturaleza genérica, los cuales aplican a toda la organización y los segundos de naturaleza específica para el teletrabajo.

Los controles adicionales aplicables al teletrabajo abarcan aquellos de los que no siempre se dispone de forma genérica ya sea en el lugar de teletrabajo o en el entorno organizativo.

En el cuadro 32, se verificaron los controles establecidos por parte de Empresa de Telecomunicaciones, susceptibles de aplicar al modelo de Teletrabajo, dando como resultado que 65 controles aplican a Teletrabajo y 51 que no genera valor agregado en esta modalidad de trabajo, a saber:

Cuadro 32. Políticas establecidas

Políticas	Descripción	Aplica a Teletrabajo?
Política de control de acceso	Acceso lógico a sistemas y servicios	SI
	Derechos y responsabilidades de acceso	SI
	Documento de aceptación a condiciones de acceso	SI
	Gestión de control de acceso (activación-inactivación)	SI
	Definir los niveles de acceso	SI
	Los privilegios de administrador del sistema - infraestructura tecnológica de la Empresa de Telecomunicaciones	SI
	Los mecanismos de entrega de contraseñas	SI
	Cambio de contraseñas al inicio de cada sistema	SI
	Seguimiento y gestión periódico al acceso del sistema	SI
	Cumplimiento con las normativas, procedimientos y buenas prácticas	SI
	Protección al acceso no autorizado	SI
	Bloqueo en estaciones de trabajo por inactividad	SI
	Acceso autorizado y controlado en las redes internas y externas de la entidad	SI
	Identificación de elementos lógicos y físicos	NO
	Restricción al acceso físico de los puertos de configuración y diagnóstico de los equipos de comunicaciones	SI
	Mecanismos de autenticación para la conexión lógica a los puertos de configuración y diagnóstica	SI
	División de las redes de la entidad	SI
	Restricción y monitoreo de conexión desde y hacia redes de la Empresa de Telecomunicaciones	SI
	Mecanismo de identificación y autenticación al acceso de sistemas de información	SI
	Autenticación y validación de cuentas de usuario y contraseñas	SI
	Cambiar contraseñas predeterminadas por el proveedor o fabricante	NO
	Denegación a la instalación o utilización de herramientas no autorizadas por la entidad	NO
	Controles de acuerdo al nivel de criticidad	SI

Cuadro 32. (Continuación)

Políticas	Descripción	Aplica a Teletrabajo?
Política Correo electrónico corporativo	Uso exclusivo de negocio	SI
	Derecho y deber a los procedimientos	SI
	Autorización y regulación a la asignación de cuentas	SI
	Lineamiento de seguridad en las contraseñas	SI
	Uso de protocolos al intercambio de correos	SI
	Denegación al uso y acceso de cuentas personales para temas laborales	SI
	Desaprobación al uso de interés personal	SI
	Restricción de entrada según categorías establecidas	SI
	Control de correo spam y uso indebido de la cuenta	SI
	Prohibición de cuentas simuladas o falsificadas	SI
	Prohibido alterar contenido del mensaje	SI
	Autorización para la revisión del contenido por parte del administrador	SI
	Manejo de registro y clasificación de información	SI
	Denegación del reenvío de información a correos personales	SI
	Uso de cuentas corporativas por parte de proveedores	SI
	Uso de la cuenta de acuerdo a su rol y lineamientos establecidos	SI
	Responsabilidad en el contenido de las cuentas	SI
Política Uso de contraseñas	Especificaciones establecidas para el uso de contraseñas	SI
	Uso personal e intransferible, información confidencial	SI
	Absoluta reserva	SI
	Las contraseñas no deben ser guardadas en ningún sistema computarizado sin cifrado.	SI
	Recomendaciones de mezcla alfa numérica	SI
	Conversión de frase a su acrónimo con símbolos	SI
	Cambiar periódicamente el método para generar contraseña	SI
	Debe ser fácil de recordar pero difícil de adivinar	SI
	No utilizar información personal, ni de trabajo, palabras de uso común.	SI

Cuadro 32. (Continuación)

Políticas	Descripción	Aplica a Teletrabajo?
Política Mantenimiento y desarrollo de aplicaciones	Cumplimiento de los controles de seguridad por parte de los terceros	NO
	Garantizar los requisitos de controles internos y seguridad para cada proyecto	NO
	Asegurar la inclusión de controles y validaciones	NO
	Garantizar la evaluación al inicio y modificación al sistema, en aspectos de seguridad y control	NO
	No deben existir usuarios de pruebas o desarrollo en ambiente de producción.	NO
	Control de cambios para la documentación y actualización en controles de seguridad	NO
	Integración al directorio corporativo y autenticación de usuarios de la Empresa de Telecomunicaciones	NO
	Validación de usuarios con el sistema de gestión humana	NO
	Gestión de funcionarios contratistas por personas de la Empresa de Telecomunicaciones	NO
	Gestión de funcionalidades y asociación de roles establecidos	NO
	Garantizar los lineamientos especificados en el framework de seguridad	NO
	Desarrolladores o proveedores deberán capacitar y apoyar al usuario en temas de seguridad	NO
	Registro al seguimiento de las actividades críticas del negocio	NO
	Asegurar el registro de logs (acceso, alarmas, operaciones, transacciones)	NO
	Control y monitoreo al nivel del código fuente correspondiente	NO
	Mecanismos de control para garantizar la calidad de los datos del negocio	NO
	Implementación en la funcionalidad del sistema la validación y el uso de los códigos definidos en las fuentes de datos	NO
	Mecanismos que permitan limitar el número de sesiones concurrentes que un usuario de aplicación y/o de base de datos puede tener.	NO
Política Red corporativa	Administración de conexiones hacia otras redes, privadas o públicas, deben ser aprobadas previamente	SI
	Asegurar las conexiones hacia y desde Internet a través del Sistema de Protección Corporativo (Firewall)	NO
	Uso de la red corporativa solo para transmitir información corporativa o de un tercero autorizado	SI
	Aprobación por el área de Seguridad sobre los nuevos servicios de Internet, que la Empresa de Telecomunicaciones llegue a proveer	NO
	Autorización de servicios por parte del área de seguridad	NO
	Validación de tráfico de red e identificación de software malicioso	SI
	La Empresa de Telecomunicaciones se reserva el derecho de negar la conectividad a páginas o servicios de Internet que considere dañinos para la infraestructura de comunicaciones o para la organización	NO

Cuadro 32. (Continuación)

Políticas	Descripción	Aplica a Teletrabajo?
Política Estaciones de trabajo	Aprobación de asignación de elementos informáticos	NO
	Aprovisionamiento de hardware y software básico	NO
	Documento de responsabilidad, condiciones y buenas prácticas para el buen uso	NO
	Características detalladas del buen uso de hardware y software de la empresa	NO
	Autorización para instalar software en una estación de trabajo	NO
	Grupo DIM (Distribución y métrica de Software) responsable del licenciamiento	NO
	Reporte de los elementos informáticos que se tiene a cargo	NO
	Desinstalación automática de software sin uso	NO
	Prohibido el uso de software que pretenda obtener información no autorizada	SI
	Software con beneficios de soporte tecnológico, suministrado corporativamente	SI
	El almacenamiento a las estaciones de trabajo solo puede usarse para información corporativa	NO
	Copia de respaldo a información corporativa almacenada en los servidores	NO
	Prohibido archivos personales en la estación de trabajo	NO
	Autorización al tener respaldo en CD	NO
	Los usuarios ya no deben compartir los recursos del PC	NO

Cuadro 32. (Continuación)

Políticas	Descripción	Aplica a Teletrabajo?
Política Uso de internet	El uso de recursos informáticos y acceso a Internet, solo para asuntos laborales	SI
	Verificación de los nuevos servicios de Internet que sean requeridos	NO
	Se prohíbe la sustitución de la identidad de un usuario en Internet o en cualquier sistema de comunicación electrónica de la empresa.	SI
	La autenticación es obligatoria para el acceso a Internet	NO
	Los usuarios no deben guardar contraseñas en sus navegadores de web	SI
	Toda comunicación a o desde las redes de la empresa se deberá efectuar a través de soluciones de telecomunicación aprobadas	SI
	Toda conexión en tiempo real con ordenadores internos de la empresa a través de Internet deberá utilizar soluciones aprobadas de la empresa y ser cifrada cuando se requiera utilizando productos aprobados	SI
	Toda comunicación entre la empresa e Internet o cualquier otra red pública se deberá efectuar a través de puertas de acceso seguras tales como firewall.	SI
	Todas las conexiones para navegar a Internet desde la red corporativa se deben realizar a través del Sistema que representa a los usuarios internos en sus solicitudes hacia Internet (proxy).	NO
	Mientras se encuentren en las instalaciones de la empresa, los usuarios no deben utilizar cuentas y servicios de proveedores de servicios de Internet (ISP) obtenidos para uso personal en su casa.	NO
	No es permitido el uso de líneas telefónicas para acceder a Internet mientras se está en las instalaciones de la empresa.	NO
	La información de la empresa que sea clasificada como secreta o confidencial solo se debe enviar a sitios de Internet de acceso público	SI
	El acceso a un sitio web determinado en Internet, la empresa puede, a su discreción, limitar o bloquear el acceso a sitios e impedir que se descarguen ciertos tipos de archivos que pueden perjudicar el servicio de la red.	NO
	La empresa usa filtro de contenido que bloque al acceso a sitios no productivos o clasificados dentro de listas negras como: pornografía, violencia, terrorismo, etc.	NO
	Desconexión de Internet al usuario que tenga un uso indebido a la red	NO
	Queda prohibido el uso indebido de Internet, Intranet, y otros servicios de Internet	NO
	Las áreas de seguridad de la empresa se reservan el derecho de examinar, en cualquier momento y sin previo aviso, archivos, marcadores, registros de sitios web visitados, configuraciones, y otras informaciones guardadas.	NO
	En el trabajo, o cuando se utilicen recursos informáticos o de redes de la empresa, se deberán respetar los derechos de propiedad intelectual en conformidad con los requisitos establecidos.	SI
	Cuando se integra información obtenida en Internet en informes internos o se utiliza para otros fines, todo el material deberá incluir etiquetas tales como "copyright, reservados todos los derechos" y la información referente a la fuente de la información.	SI

Cuadro 32. (Continuación)

Políticas	Descripción	Aplica a Teletrabajo?
Política Contratistas	Cada contratista debe disponer de los equipos de cómputo que requiera para el desempeño de las actividades y funciones para las cuales fue contratado.	SI
	En lo posible las actividades deben ser desempeñadas en las instalaciones del contratista y solo ejecutar en las instalaciones de la Empresa de Telecomunicaciones las actividades que sean estrictamente necesarias, como por ejemplo pruebas y puesta en funcionamiento.	NO
	Para los casos que sea indispensable la presencia de los contratistas en las instalaciones de la Empresa de Telecomunicaciones, es obligación que el supervisor de cada contrato envíe a través de correo la información de los equipos que requieren conectarse a red, con el fin de iniciar el alistamiento de los equipos	NO
Política Antivirus	No aceptar vía e-mail los archivos ejecutables con extensiones tales como EXE, COM, BAT, REG, etc., pueden causar una modificación ó daño a los archivos de la estación de trabajo con solo abrirlos.	SI
	No descargar archivos de sitios desconocidos o fuentes sospechosas. Deben visitar sitios de empresas conocidas con las que se mantienen relaciones laborales u organizaciones que se dedican a temas específicos con reconocimiento a nivel mundial	SI
	No se permite a los usuarios la erradicación de virus. En caso de infección se debe contactar a la mesa de servicio	NO
	Se debe tener implementado un sistema corporativo de antivirus a para estaciones de trabajo	SI

Fuente: Empresa de Telecomunicaciones, adaptación por el autor

8. CONTROLES PROPUESTOS PARA TELETRABAJO

El teletrabajo requiere además de un análisis detallado, realizar su debida valoración y tratamiento al riesgo. Como parte del proceso y éxito a la implementación de la modalidad del teletrabajo, es importante tener en cuenta los controles para que se pueda garantizar el adecuado ejercicio del teletrabajo.

Como parte de apoyo y orientación a los procesos y procedimientos de la entidad, se realizó un análisis de los controles y políticas existentes, con base en lo anterior, se referencia los controles que se deben tener para la modalidad del teletrabajo y así lograr identificar los elementos a incorporar[23].

En cuadro 33, se muestra los controles que se deben tener en cuenta para la modalidad del teletrabajo, de acuerdo a una clasificación dada:

[23] NIST SP 800-46 Guide to Enterprise Telework and Remote access security

Cuadro 33. Controles para la modalidad del teletrabajo

CONTROLES			
	Descripción	**Existente**	**No Existente**
Administrativos	Política de seguridad para el teletrabajo		X
	Desarrollar e implementar un acuerdo de teletrabajo		X
	Administrar solicitudes y autorizar teletrabajadores		X
	Aprobación de ubicaciones remotas		X
	Mantener la documentación adecuada del servicio de teletrabajo		X
	Supervisar los registros de auditoria		X
	Proporcionar soporte técnico a los teletrabajadores		X
	Registro de incidentes	X	
El teletrabajador	Desarrollar un código de conducta para el teletrabajo		X
	Establecer directrices para el uso de información sensibles	X	
	Establecer directrices para el uso de los ordenadores no relacionado con el trabajo	X	
	Establecer directrices para el uso de redes inalámbricas		X
	Establecer directrices para el uso de software anti-malware y Firewall		X
	Establecer directrices para la toma de las copias de seguridad		X
	Establecer directrices para el uso de dispositivos de datos portátiles		X
	Establecer directrices para el uso de Internet		X
	Establecer directrices para utilizar el correo electrónico	X	
	Establecer directrices para el uso de medios de autenticación		X
	Establecer pautas para prevenir el robo		X
	Establecer directrices para fijar la ubicación remota		X
	Proporcionar copias del código y las directrices a los teletrabajadores		X
	Distribuir material de sensibilización		X
	Definir estrategia de contingencia en ausencia de Teletrabajador		X
	Proporcionar formación de conciencia de seguridad		X

Cuadro 33. (Continuación)

CONTROLES			
	Descripción	**Existente**	**No Existente**
Instalaciones	Asegurar Condiciones locativas y de entorno		X
	Asegurar la seguridad física de los equipos de trabajo		X
	Asegurar condiciones ergonómicas		X
	Asegurar condiciones ambientales		X
	Conocer procedimientos de acción al caso de riesgo eléctrico y de incendio	X	
El equipo teletrabajo	Implementar una configuración técnica estándar		X
	Verificar las características mínimas para el equipo de cómputo y conexión a internet		X
	Utilice hardware y software fiable		X
	Preinstalar y preconfigurar software		X
	Implementar software anti-malware		X
	Implementar un servidor de seguridad personal (firewall personal)		X
	Descargar e instalar automáticamente las actualizaciones y parches		X
	Implementar notificaciones de advertencia en la pantalla		X

Cuadro 33. (Continuación)

CONTROLES			
	Descripción	Existente	No Existente
La conexión a Internet	Implementar un adecuado procedimiento de log-on	X	
	Implementar un mecanismo de autenticación	X	
	Asegurar el uso de contraseñas seguras	X	
	Asegurar el cambio continuo de la contraseña		X
	Asegurar la configuración de arranque al computador		X
	Implementar bloqueo de acceso automático		X
	Cifrar automáticamente los datos en el disco duro		X
	Implementar modo a prueba de fallos automática en caso de escasez de energía		X
	Implementar software de bloqueo del dispositivo		X
	Implementar un filtro de URL		X
	Impedir la instalación de software no autorizado		X
	Almacenar de forma segura las contraseñas y claves criptográficas		X
	Implementar software de seguimiento antirrobo		X
	Respaldo de datos automático		X
	Manejo de Proveedores de acceso a Internet	X	
	Proporcionar canales de Internet a diferentes centrales a modo de contingencia	X	
	Prevenir el secuestro de conexiones		X
	Terminar automáticamente conexiones no utilizadas		X
	Restringir el número de conexiones abiertas simultáneamente	X	
Acceso remoto a la red corporativa de la empresa	Implementar y mantener el software anti-malware y cortafuegos	X	
	Implementar un adecuado procedimiento de log-on	X	
	Implementar un mecanismo de autenticación	X	
	Asegurar el uso de contraseñas seguras	X	
	Asegurar el cambio continuo de la contraseña	X	
	Implementar los derechos de acceso teletrabajador		X
	Restringir el acceso a ordenadores autorizados	X	
	Aplicar técnicas de balanceo de carga	X	

Fuente: NIST SP 800-46 Guide to Enterprise Telework, adaptación por el autor

Con el anterior cuadro de control, se menciona cada uno de ellos con una breve explicación:

8.1 CONTROL ADMINISTRATIVO

Su aplicación es fundamental como parte inicial a los controles de seguridad de la información, dado a que las medidas y procedimientos deben estar en forma coordinada y apoyada por la administración. Dentro de estos controles están:

- Política de seguridad para el teletrabajo: La política de seguridad para el teletrabajo, debe estar desarrollada, implementada y aprobada en la organización, deberá evaluarse de forma constante para su validez.
- Desarrollar e implementar un acuerdo de teletrabajo: El acuerdo debe estar documentado para garantizar las responsabilidades y obligaciones del teletrabajador, con la precisión de información sobre la seguridad de la información, riesgos y tratamiento a ellos.
- Administrar solicitudes y autorizar teletrabajadores: El interesado debe presentar formalmente la solicitud, se evaluará utilizando un procedimiento detallado de la solicitud y se aprobara o denegará de acuerdo a la decisión del responsable.
- Aprobación de ubicaciones remotas: La ubicación del teletrabajador debe ser revisada y aprobada de acuerdo a unas medidas de seguridad (físicas y tecnológicas), además se recomienda realizar una evaluación periódica.
- Mantener la documentación adecuada del servicio de teletrabajo: Es indispensable conservar y actualizar toda documentación del proceso.
- Supervisar los registros de auditoría: Seguimiento y análisis a los registros de auditoría al acceso remoto, de forma contínua.
- Proporcionar soporte técnico a los teletrabajadores: El servicio de soporte técnico debe estar presente 7x24, y solucionar cualquier incidente que se presente en una forma rápida y eficaz.
- Registro de incidentes: Incidentes que se presenten como pérdida de energía, mal funcionamiento, caídas del sistema, errores generados y brechas de seguridad, deben ser reportados de forma inmediata para su solución oportuna.

8.2 **CONTROL DEL TELETRABAJADOR**

Su control es parte esencial en el desarrollo y ejecución del proceso, y así prevenir riesgos ocasionados por la falta de control y seguimiento. A continuación se mencionan varios de estos controles:

- Desarrollar un código de conducta para el teletrabajo: Elaboración de una serie de reglas de conducta y responsabilidades del teletrabajador, con respecto a la seguridad de la información
- Establecer directrices para el uso de información sensibles: Instrucciones establecidas al manejo de la información y datos sensibles de la organización.
- Establecer directrices para el uso de los ordenadores no relacionado con el trabajo: Prohibición al uso de computadoras de teletrabajo no relacionadas con el trabajo, se puede exponer a un riesgo de seguridad.
- Establecer directrices para el uso de redes inalámbricas: Se debe establecer condiciones de uso de acuerdo a la aprobación o negación del servicio, considerando los riesgos de seguridad.
- Establecer directrices para el uso de software anti-malware y Firewall: Instrucciones de uso del software, instalación y configuración en los equipos de teletrabajo.
- Establecer directrices para la toma de las copias de seguridad: Garantizar el respaldo de la información con mecanismos de cifrado para salvaguardar la confidencialidad y uso de software de confianza.
- Establecer directrices para el uso de soportes de datos portátiles: Establecer instrucciones de alerta, para el uso de datos portátiles con origen desconocido o no confiables.
- Establecer directrices para el uso de Internet: El teletrabajador debe seguir una serie de instrucciones como el no acceso a sitios web desconocidos, descargas no confiables, etc.
- Establecer directrices para utilizar el correo electrónico: Uso del correo electrónico por los teletrabajadores, deberán seguir instrucciones establecidas como es el manejo de los archivos adjuntos desconocidos, utilizar información confidencial sin cifrado, uso de software anti-malware.
- Establecer directrices para el uso de medios de autenticación: Los teletrabajadores deberán seguir una serie de instrucciones establecidas, al uso adecuado de las credenciales de acceso como por ejemplo, cambio de contraseña de forma periódica, uso de contraseñas fuertes, confidencialidad y reserva.
- Establecer pautas para prevenir el robo: Directrices que indican las diferentes formas de prevenir el robo o pérdida de equipos utilizados para el teletrabajo y la información que contiene. Para los equipos se debe tener precaución en

lugares públicos, usar protección al dispositivo móvil, uso de caja de seguridad, aislarlo a temperaturas fuertes. En cuanto a la información, no procesar información confidencial en lugares públicos, realizar el debido manejo de conexión, cifrar la información.

- Establecer directrices para fijar la ubicación remota: Directrices en relación con la seguridad física para protección de los equipos de teletrabajo, previniendo daño de entorno.
- Proporcionar copias del código y las directrices a los teletrabajadores: Los teletrabajadores deben recibir una copia del código de conducta y directrices establecidas, al inicio del proceso y al realizar alguna modificación.
- Distribuir material de sensibilización: Se debe entregar material sobre los riesgos de seguridad asociados a la modalidad del teletrabajo, realizar capacitaciones, campañas de sensibilización y recomendaciones sobre las buenas prácticas.
- Proporcionar formación de conciencia de seguridad: En forma periódica se debe capacitar sobre el uso correcto del sistema, conocer sus responsabilidades y obligaciones en la modalidad del teletrabajo, comprender los riesgos de seguridad que se puedan presentar y cómo manejarlos.

8.3 CONTROL DE LAS INSTALACIONES

Como principal objetivo del área de tecnología de información y comunicaciones, es el control físico de las instalaciones de la organización, las cuales se mencionan algunas a continuación:

- Asegurar Condiciones locativas y de entorno: Se debe garantizar las condiciones de ubicación y entorno para evitar intrusos.
- Asegurar la seguridad física de los equipos de trabajo: Garantizar que los equipos asignados a teletrabajo, estén seguros físicamente.
- Asegurar condiciones ergonómicas: Comprobar el sitio de teletrabajo, con las recomendaciones que realiza la ARL (Administradora de Riesgos Laborales)
- Asegurar condiciones ambientales: Verificar que las condiciones de teletrabajo, pueda aplicar un mecanismo de protección.
- Conocer procedimientos de acción al caso de riesgo eléctrico y de incendio: Capacitación al personal sobre los tipos de riesgos y la acción a realizar.

8.4 CONTROL EQUIPO TELETRABAJO

Es elemental en los controles de seguridad de la información y uso de los equipos de trabajo, incluyendo el seguimiento a los equipos que los teletrabajadores utilicen.

- Implementar una configuración técnica estándar: Se recomienda utilizar una configuración estándar a los equipos del teletrabajo, para mantener un modelo de verificación.
- Verificar las características mínimas para el equipo de cómputo y conexión a internet: Para garantizar un buen funcionamiento del equipo de cómputo, debe tener las características técnicas mínimas y la conexión a internet como requisito establecido por la entidad.
- Utilice hardware y software fiable: La fiabilidad en el hardware y software, utilizado por los teletrabajadores debe estar garantizado para un correcto funcionamiento.
- Preinstalar y pre configurar software: Los equipos de teletrabajo deberán tener una preinstalación y configuración en forma correcta (firewall personal, control de acceso lógico, sistema operativo, etc.), para evitar la alteración de cambios que puedan afectar la seguridad del equipo e información.
- Implementar software anti-malware: Como prevención de los programas maliciosos, virus informáticos, se solicita instalar en el equipo del teletrabajador, un software antimalware.
- Implementar un servidor de seguridad personal (firewall personal): Un firewall personal proporciona un cierto nivel de detección de intrusos, se debe tener instalado en los equipos de los teletrabajadores, para permitir controlar la comunicación que se genera, y así evitar una intrusión.
- Descargar e instalar automáticamente las actualizaciones y parches: Como forma de mantener protegido el equipo de cómputo del teletrabajador, se recomienda realizar las actualizaciones del sistema operativo y parches de software requeridos.
- Implementar notificaciones de advertencia en la pantalla: Notificaciones en la pantalla del equipo de cómputo, apoya como medida de prevención y advertencia sobre los accesos no autorizados, y permite observar recomendaciones de seguridad de la información**.**

8.5 CONTROL A LA CONEXIÓN A INTERNET

Su aplicación y competencia del área de tecnología y seguridad de la información, para garantizar el buen uso y protección de los datos manejados en la organización.

- Implementar un adecuado procedimiento de log-on: En el procedimiento debe contener una serie de indicaciones cómo: validación de datos al inicio de sesión, limitar el número innecesarios intentos de inicio de sesión permitido, ocultar caracteres de la contraseña, limitar el tiempo máximo y mínimo permitido.
- Implementar un mecanismo de autenticación: El mecanismo de autenticación debe garantizar la identidad del usuario, validar contraseñas y cumplir los lineamientos de uso.
- Asegurar el uso de contraseñas seguras: Se debe asegurar que las contraseñas utilizadas, cumplan con unas condiciones fuertes como longitud, combinación, limitación de consecutivos, etc.
- Asegurar el cambio continuo de la contraseña: Dentro de los mecanismos de seguridad para la administración de contraseñas, se debe tener en cuenta el cambio periódico de las contraseñas, fijando tiempo, reutilización, inicio por primera vez, etc.
- Asegurar la configuración de arranque al computador: Se debe garantizar la configuración de arranque del equipo de teletrabajador, por medio determinado como el disco duro y evitar el inicio de otros medios no confiables.
- Implementar bloqueo de acceso automático: Se debe implementar el bloqueo de acceso automático para prevenir la intrusión al momento de que el equipo del teletrabajador se encuentre en un periodo de tiempo sin uso.
- Cifrar automáticamente los datos en el disco duro: La información utilizada por el teletrabajador es de vital importancia para la organización, por ello se debe implementar un mecanismo de cifrado automático como prevención de acceso no autorizado.
- Implementar modo a prueba de fallos automática en caso de escasez de energía: La escasez de energía puede apagar bruscamente el equipo de cómputo del teletrabajador y conducir a la pérdida de los datos, se recomienda configurar de forma automática al modo a prueba a fallos de alimentación.
- Implementar software de bloqueo del dispositivo: Se debe controlar el acceso de los dispositivos externos a los equipos de cómputo del teletrabajador, y así prevenir posibles daños.
- Implementar un filtro de URL: Se debe asegurar con un filtro de URL, el bloqueo de páginas web no autorizadas para el teletrabajador.

- Impedir la instalación de software no autorizado: El equipo de cómputo del teletrabajador debe estar previamente configurado para evitar que se instale software no autorizado.
- Almacenar de forma segura las contraseñas y claves criptográficas: Se debe asegurar que las contraseñas utilizadas por el teletrabajador, sean almacenadas de forma segura y utilizar el mecanismo de cifrado, adicionalmente desactivar el almacenamiento automático.
- Implementar software de seguimiento antirrobo: Software de seguimiento antirrobo debe estar instalado en los equipos de cómputo del teletrabajador, para ayudar a su recuperación en caso de robo.
- Respaldo de datos automático: Es recomendable utilizar respaldos de información en forma automática a los equipos de cómputo de los teletrabajadores, cuando realizan una conexión remota.
- Manejo de Proveedores de acceso a Internet: Deberá estar definido en acuerdos formales, el acceso a Internet requeridos por los proveedores y establecer un estándar limitado de acceso.
- Proporcionar múltiples líneas a diferentes centrales telefónicas: Como medida a la falla de una línea o central telefónico, se recomienda tener una infraestructura de comunicaciones alterna.
- Prevenir el secuestro de conexiones: Mecanismos de prevención para mitigar el riesgo de seguridad relacionada con el acceso no autorizado a las conexiones de comunicación.
- Terminar automáticamente conexiones no utilizadas: Métodos que permite evitar un acceso no autorizado por tener conexiones abiertas.
- Restringir el número de conexiones abiertas simultáneamente: Se debe garantizar el control de las conexiones abiertas en simultánea, limitando el acceso y garantizando la disponibilidad.

8.6 CONTROL AL ACCESO REMOTO A LA RED CORPORATIVA

Su aplicación y responsabilidad del área de tecnología y seguridad de la información, para garantizar la protección de los datos que se transfieren durante la conexión, a continuación se mencionan:

- Implementar y mantener el software anti-malware y cortafuegos: Se debe garantizar la configuración y actualización del software anti-malware y cortafuegos.
- Implementar los derechos de acceso teletrabajador: Garantizar las políticas de acceso remoto a las aplicaciones e información otorgados en vigencia a la modalidad del teletrabajo, realizar seguimiento al acceso.

- Restringir el acceso a ordenadores autorizados: Se debe limitar las condiciones de acceso a los equipos de cómputo del teletrabajador.
- Aplicar técnicas de balanceo de carga: Se recomienda dividir en forma automática el acceso remoto de los usuarios en el servidor de aplicaciones

9. PLAN PARA TRATAMIENTO DEL RIESGO

Basado en la información analizada respecto de la lista de amenazas y controles existentes se realizó un plan para el tratamiento del riesgo, teniendo en cuenta las siguientes consideraciones:

- Para el área de la mesa de ayuda para grandes clientes de la Empresa de Telecomunicaciones, es inaceptable y con impacto grave los eventos que puedan afectar la confidencialidad de la información de la empresa y de sus clientes debido a que se incurriría en una violación de legislación aplicable, se faltaría a cláusulas de confidencialidad para manejo de información crítica de otras empresas y puede resultar en afectación de servicios, robo o cambio de información, con implicaciones legales, económicas y de reputación de la organización

- Los activos más utilizados dentro de los procesos y actividades realizados en la labor diaria son correspondientes a los grupos de Personas (Teletrabajador), servicios (Conexión a Internet) y hardware (Instalaciones y equipo de trabajo)

- Con respecto a Impacto, la criticidad más alta corresponde al grupo de activos de hardware (Instalaciones y equipo de trabajo)

- La probabilidad más alta de ocurrencia se presenta en los activos que corresponden al grupo de servicios (Conexión a Internet, acceso a la red corporativa y correo)

- Se encuentra en la zona de alto riesgo los eventos que puedan afectar la disponibilidad de los activos, seguida de aquellos eventos que pueden afectar la confidencialidad

- Se deben realizar el manejo de riesgos según su prioridad en el siguiente orden:

Disponibilidad:

- Malos tiempos de respuesta al cliente debido a problemas en la disponibilidad de los activos, problemas lentitud.
- Falta de documentación y seguimiento de actividades realizadas debido a problemas en la disponibilidad de los activos.
- Incumplimiento en actividades asignadas debido a problemas en la disponibilidad de los activos.

Confidencialidad:

- Revelación de información crítica de la Empresa de Telecomunicaciones o del cliente por falla en manejo de información confidencial.

Integridad:

- Información confusa o errónea al cliente debido a falta de integridad de la información que se maneja y problemas en la disponibilidad de elementos para la comunicación.
- Comunicación deficiente con áreas especializadas para solución de fallas o respuesta a requerimientos, debido a la falta de integridad de la información que se maneja, problemas en la disponibilidad de elementos para la comunicación.

Basado en la información recolectada, se realizó la identificación de amenazas, y los controles existentes y propuestos a la luz de las características de disponibilidad, confidencialidad e integridad de la información, las cuales se pueden advertir en el siguiente cuadro:

Cuadro 34. Amenazas y controles que implican la disponibilidad

DISPONIBILIDAD			
Activo	**Amenaza**	**Control**	**Estrategia de tratamiento**
Teletrabajador	El Ingeniero no se encuentra disponible para el proceso.	• Definir estrategia de contingencia en ausencia de Teletrabajador	Reduce
Instalaciones	Fuente de alimentación no fiable	• Asegurar Condiciones locativas y de entorno • Asegurar la seguridad física de los equipos de trabajo • Conocer procedimientos de acción al caso de riesgo eléctrico y de incendio	Reduce
Conexión a Internet	Conexión a Internet no disponible	• Aprobación de ubicaciones remotas • Proporcionar canales de Internet a diferentes centrales a modo de contingencia • Manejo de Proveedores de acceso a Internet • Implementar modo a prueba de fallos automática en caso de escasez de energía	Reduce
	Conexión a Internet no fiable o lento	• Manejo de Proveedores de acceso a Internet • Proporcionar canales de Internet a diferentes centrales a modo de contingencia	Reduce
Equipo	Equipo teletrabajo no es adecuado para el teletrabajo	• Implementar una configuración técnica estándar • Verificar las características mínimas para el equipo de cómputo y conexión a internet	Reduce
	Acceso a Internet, mal funcionamiento del dispositivo	• Verificar las características mínimas para el equipo de cómputo y conexión a internet • Preinstalar y pre configurar software • Descargar e instalar automáticamente las actualizaciones y parches	Reduce
	Mal funcionamiento de software de comunicaciones	• Preinstalar y pre configurar software	Reduce

Fuente: Autores

Cuadro 35. Amenazas y controles que implican la confidencialidad

CONFIDENCIALIDAD			
Activo	**Amenaza**	**Control**	**Estrategia de tratamiento**
Teletrabajador	La divulgación de la información de inicio de sesión	• Desarrollar e implementar un acuerdo de teletrabajo • Desarrollar un código de conducta para el teletrabajo • Establecer directrices para el uso de información sensibles • Proporcionar copias del código y las directrices a los teletrabajadores • Distribuir material de sensibilización • Proporcionar formación de conciencia de seguridad	Reduce
	La elección de contraseñas débiles	• Para el acceso a la red corporativa y los sistemas de la Empresa de Telecomunicaciones, el teletrabajador debe seguir las normativas definidas por la entidad en la política de control de acceso, y se recomienda para el manejo de contraseñas en el ordenador y de cifrado de datos tener en cuenta la Política de Uso de Contraseñas	Reduce
	Conexión del equipo teletrabajo a las redes públicas	• Establecer directrices para el uso de redes inalámbricas: No se deben utilizar conexiones poco confiables (conexiones Wi-Fi abiertas, redes públicas de hoteles, bibliotecas, locutorios, etc.) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL. No basta con que la red tenga contraseña para conectar ya que los propietarios de la red podría monitorizar el tráfico, por lo que se debe aplicar una capa extra de cifrado.	Reduce
	Equipos de teletrabajo en daño en manos de terceros	• Distribuir material de sensibilización • Proporcionar formación de conciencia de seguridad	Reduce
	El uso de los ordenadores de teletrabajo por parte de terceros	• Distribuir material de sensibilización • Proporcionar formación de conciencia de seguridad	Reduce

Cuadro 35. (Continuación)

CONFIDENCIALIDAD			
Activo	**Amenaza**	**Control**	**Estrategia de tratamiento**
Instalaciones	Inspección de la información a través de vistas	• Aprobación de ubicaciones remotas • Establecer directrices para fijar la ubicación remota • Asegurar Condiciones locativas y de entorno • Asegurar la seguridad física de los equipos de trabajo	Reduce
Conexión a Internet	La inspección no autorizada de datos en tránsito	• Cifrar automáticamente los datos en el disco duro • Almacenar de forma segura las contraseñas y claves criptográficas	Reduce
	Secuestro de la conexión	• Prevenir el secuestro de conexiones	Reduce
	Conexiones no utilizadas permanecen abiertas	• Restringir el número de conexiones abiertas simultáneamente	Reduce

Cuadro 35. (Continuación)

CONFIDENCIALIDAD			
Activo	**Amenaza**	**Control**	**Estrategia de tratamiento**
Equipo	Control de acceso lógico anulado en el ordenador de teletrabajo	• Implementar software anti-malware • Implementar un servidor de seguridad personal (firewall personal) • Implementar notificaciones de advertencia en la pantalla • Descargar e instalar automáticamente las actualizaciones y parches	Reduce
	Las características de seguridad no configurados correctamente	• Implementar una configuración técnica estándar • Utilice hardware y software fiable • Preinstalar y pre configurar software • Implementar software anti-malware • Implementar un servidor de seguridad personal (firewall personal) • Descargar e instalar automáticamente las actualizaciones y parches	Reduce
	Descubrimiento de información de inicio de sesión que se almacena en el ordenador del teletrabajo	• Implementar un servidor de seguridad personal (firewall personal) • Implementar notificaciones de advertencia en la pantalla • Utilice hardware y software fiable	Reduce
	Las claves de cifrado almacenadas en el ordenador teletrabajo comprometidas	• Implementar un servidor de seguridad personal (firewall personal) • Implementar notificaciones de advertencia en la pantalla • Utilice hardware y software fiable	Reduce
Acceso red corporativa	Teletrabajador tiene demasiados derechos de acceso a la red corporativa de la empresa de forma remota	• Se deben seguir los lineamientos de la Política Red corporativa y la Política de control de acceso ya definidas por la entidad	Reduce

Fuente: Autores

Cuadro 36. Amenazas y controles que implican la integridad

INTEGRIDAD			
Activo	**Amenaza**	**Control**	**Estrategia de tratamiento**
Teletrabajador	La elección de contraseñas débiles	• Para el acceso a la red corporativa y los sistemas de la Empresa de Telecomunicaciones, el teletrabajador debe seguir las normativas definidas por la entidad en la política de control de acceso, y se recomienda para el manejo de contraseñas en el ordenador y de cifrado de datos tener en cuenta la Política de Uso de Contraseñas	Reduce
	Introducción de malware a través de Internet o correo electrónico	• Establecer directrices para el uso de software anti-malware y Firewall • Establecer directrices para utilizar el correo electrónico • Distribuir material de sensibilización • Proporcionar formación de conciencia de seguridad	Reduce
	La introducción de malware de soportes de datos portátiles	• Establecer directrices para el uso de software anti-malware y Firewall • Establecer directrices para el uso de soportes de datos portátiles • Distribuir material de sensibilización • Proporcionar formación de conciencia de seguridad	Reduce
	Negligencia de importantes actividades de mantenimiento	• Desarrollar un código de conducta para el teletrabajo • Proporcionar formación de conciencia de seguridad	Reduce
	La carga de software dañino	• Establecer directrices para el uso de Internet • Establecer directrices para el uso de software anti-malware y Firewall	Reduce
	Cambios inapropiados en la configuración del software	• Desarrollar un código de conducta para el teletrabajo • Establecer directrices para el uso de los ordenadores	Reduce

Cuadro 36. (Continuación)

INTEGRIDAD			
Activo	**Amenaza**	**Control**	**Estrategia de tratamiento**
Conexión a Internet	Secuestro de la conexión	• Impedir la instalación de software no autorizado • Prevenir el secuestro de conexiones • Terminar automáticamente conexiones no utilizadas • Restringir el número de conexiones abiertas simultáneamente	Reduce
	Conexiones no utilizadas permanecen abiertas	• Terminar automáticamente conexiones no utilizadas • Restringir el número de conexiones abiertas simultáneamente	Reduce
Equipo	Protección contra malware inadecuada	• Implementar software anti-malware • Utilice hardware y software fiable	Reduce

Fuente: Autores

10. CONCLUSIONES

Como resultado del presente trabajo de investigación, se muestran los beneficios y ventajas que se tiene al implementar el teletrabajo en el área de mesa de ayuda, y se da el hecho de que el teletrabajo optimiza los recursos de la Empresa de Telecomunicaciones, contribuye a una mayor productividad, eficiencia y menor ausentismo, genera confianza en relación empleador-teletrabajador contribuyendo en consecuencia al mejoramiento del clima organizacional, aumenta el sentido de pertenencia, se realiza una mayor retención de trabajadores y permite la autogestión por parte de los mismos, no sin olvidar los beneficios que genera al teletrabajador, entre los cuales se destacan la autonomía, libertad y flexibilidad en el desarrollo de sus actividades; así como la posibilidad de compartir más tiempo con la familia, y mejorar en consecuencia su calidad de vida, el ahorro en tiempo y dinero propio de desplazamientos, en este último generando una reducción de costos para la organización y para el teletrabajador.

Como se menciona en el capítulo 4.4, también es importante indicar que basado en el levantamiento de información de los procesos, cargos, y perfiles realizado en el capítulo 6, la adopción de dicha modalidad de trabajo no implica cambio en los procesos, cargos o perfiles actualmente definidos para las actividades a desempeñar por parte de los Ingenieros de soporte de la mesa de ayuda de la Empresa de Telecomunicaciones, adicionalmente se resalta en el área el control de gestión a través de una herramienta tecnológica y una mayor correspondencia e identidad entre intereses del teletrabajador y de la Empresa de Telecomunicaciones, condición que se suma a las ventajas anteriormente mencionadas.

Como otro efecto positivo aparejado, se determina que orientar a la modalidad de teletrabajo la operación de la mesa de ayuda de grandes clientes de la Empresa de Telecomunicaciones es viable y se advierte como una opción con ventajas y beneficios positivos para la organización, mientras se tomen medidas y controles de seguridad de la información que mantengan y ratifiquen los objetivos establecidos por parte de la Empresa de Telecomunicaciones para la Mesa de Ayuda; esta conclusión se fundamentó a partir de un proceso de corroboración de la pregunta formulada como punto de partida y descriptor de la problemática, realizado mediante la aplicación, análisis y estudio de las técnicas de investigación utilizadas, en donde, en ejercicio de la observación, se identificó como antecedente la realización de un piloto y consideraciones que dan cuenta de la conciencia sobre los beneficios positivos de orientar este proceso al teletrabajo.

Una vez cimentado el anterior pilar como punto de apoyo, se orientó el desarrollo de la propuesta, realizado en el contexto de la administración de riesgos con énfasis en el sistema de seguridad de la información, y a la luz del desarrollo conceptual del teletrabajo y los aspectos y atributos propios de un sistema seguro como lo son: la confiabilidad, integridad y disponibilidad, a constituir el presente como un documento de referencia y apoyo, al nivel directivo al momento de tomar la decisión definitiva de volcar la mesa de ayuda hacia esta modalidad.

Su principal aporte lo constituye el hecho de que trasciende las iniciativas realizadas al interior de la organización en este sentido, avanza y complementa estos esfuerzos, al incorporar la propuesta de estrategia de seguridad de la información con la observancia de condiciones seguras, elemento este, esencial para superar la restricción encontrada en su momento respecto de la incertidumbre sobre operar de manera segura en esta modalidad, factor que se convirtió en un inhibidor que truncó esta iniciativa en la Empresa de Telecomunicaciones.

Del mismo modo, incorpora el análisis de riesgo de la infraestructura operacional, de telecomunicaciones, y de servicio disponibles como base para el desarrollo de la propuesta, advirtiendo las brechas existentes entre la efectividad, aplicación y suficiencia de los controles propios de estas infraestructuras, y planteando aquellos controles requeridos para completar una operación de Teletrabajo en condiciones seguras y precedida bajo el enfoque de la norma ISO 31000.

Apoyado en la recolección de información de los procesos y prioridades de la mesa de ayuda de la Empresa de Telecomunicaciones, la situación actual con respecto a las pruebas preliminares de teletrabajo realizadas en el área y las herramientas tecnológicas disponibles suministradas y administradas por la organización; se deben tener en cuenta en el desarrollo de políticas y controles mencionados la confidencialidad y la disponibilidad de la información como características críticas en el cumplimiento de los objetivos del área, brindando especial atención a la protección y regulación de los activos relacionados con el teletrabajador, el hardware utilizado y los servicios que actúan en la ejecución de Teletrabajo en el modelo actual, ya que en análisis realizado se encuentran éstos con mayor porcentaje de utilización, mayor criticidad de impacto y probabilidad de ocurrencia.

Teniendo en cuenta que en la solución actual la conexión a Internet y el equipo de trabajo son propiedad y administrados por el teletrabajador, los controles inicialmente deben enfocarse o encaminarse a la capacitación del mismo, la

creación de conciencia de seguridad de la información y el seguimiento y control por parte de la organización al aseguramiento de los equipos utilizados en la jornada de teletrabajo; para este último punto es necesario tener en cuenta consideraciones jurídicas y legales como es el acuerdo al Artículo 57 del Código Sustantivo del Trabajo que establece como excepción en el numeral 1, que con respecto a los instrumentos adecuados y las materias primas necesarias para la realización de las labores, las partes pueden pactar que el empleado suministre el equipo informático; en ese caso, el empleador debe compensar el costo que le generó esa herramienta al trabajador, o entregar una prima extra en compensación por la utilización de las herramientas tecnológicas para fines laborales; para tal fin al ser aprobada esta propuesta por parte del área directiva será preciso realizar un alineamiento entre las áreas legal, financiera, de infraestructura y seguridad con el fin de determinar los cambios a realizar y procesos a definir para la inclusión de Teletrabajo como modelo laboral en el área de mesa de ayuda.

En consecuencia, y examinado a la luz de un enfoque teórico de organización inteligente, construye conocimiento al generar valor agregado, y resolver con la propuesta de la estrategia de seguridad, la incertidumbre e inquietudes identificadas y constituidas en barreras de las iniciativas sobre el particular, por ende, cumple con la expectativas de la Empresa de Telecomunicaciones en particular del área de la mesa de ayuda, y pretende ser el documento inductor en la toma de decisión de la alta dirección sobre orientar a modalidad de teletrabajo su mesa de ayuda de grandes clientes.

Si bien es cierto, la orientación del trabajo se centró en la administración de los riesgos a proteger la información de la Empresa de Telecomunicaciones, en lo que concierne a la salvaguarda de los accesos y servicios, también lo hizo direccionada a la protección de la información de los clientes que viaja a través de la red y se encuentra contenida en los servicios tecnológicos ofrecidos por la Empresa de Telecomunicaciones, que al orientarla a la modalidad de trabajo podría constituirse en una gran amenaza por la condición inherente de la información al ser gestionada en el marco de un contrato de confidencialidad.

Y es precisamente en este aparte, en donde la propuesta adquiere relevancia determinante; es decir, no solo se está orientando un proceso cualquiera a la modalidad de teletrabajo, sino que adicionalmente, se está proponiendo realizarlo con la ejecución de una estrategia de seguridad que fortalece los dispositivos de control y de esta manera, administra los riesgos propios de gestionar información personal y confidencial de los grandes clientes de la Empresa de Telecomunicaciones. En ese orden de ideas, ratifica su condición de viabilidad,

contesta la pregunta realizada en el planteamiento del problema del presente trabajo, suma y aporta viabilidad tecnológica, operacional y de seguridad en la gestión de la información.

La decisión de cambiar el modelo de operación convencional a un esquema soportado en el teletrabajo, supone un cambio en el paradigma que como se realiza la métrica para medir la productividad de los trabajadores. Pasar de una medición orientada en horas y días hombre a una basada y orientada a resultados, situación que exigirá del acompañamiento en un sistema de control de gestión que permita medir de manera efectiva el desempeño y la productividad en la modalidad de teletrabajo.

11. RECOMENDACIONES

Como recomendaciones derivadas del presente trabajo y una vez advertida y decidida la ejecución de orientarse a la modalidad de teletrabajo, se plantean las siguientes:

- Socializar los beneficios e impacto positivo del presente documento en primera instancia, a la alta dirección responsable de la toma de la decisión en torno a orientar a la modalidad de teletrabajo la mesa de ayuda de grandes clientes de la Empresa de Telecomunicaciones, y en segunda y basado en la determinación tomada a los integrantes de la mesa de ayuda.

- Implementar la estrategia y políticas de gestión del riesgo de la información para proteger la información para la modalidad del teletrabajo del proceso de mesa de ayuda.

- Establecer mecanismos que demuestren el compromiso y voluntad de la alta dirección para brindar apoyo y respaldo a los líderes de los procesos de gestión del riesgo de TI y seguridad en la implementación de los aspectos sugeridos con la presente propuesta.

- Establecer mecanismo de coordinaciones entre las diferentes dependencias de la Empresa de Telecomunicaciones para la ejecución compartida de las acciones que derive la propuesta, capacitar a los diferentes involucrados en el proceso, y realizar seguimiento periódico a la ejecución del cronograma establecido.

REFERENCIAS BIBLIOGRÁFICAS

A Colombia llega la Feria Internacional del Teletrabajo. Disponible en: http://www.mintrabajo.gov.co/julio-2012/711-a-colombia-llega-la-feria-internacional-del-teletrabajo.html

ANDREU, R., RICART, J. E. y VALOR, J. (1996): Estrategia y Sistemas de Información, 2ª Edición, McGraw-Hill, pag. 13.

Bogotá es una Ciudad para el Teletrabajo: Jack Nilles. Disponible en: http://www.colombiadigital.net/teletrabajo/item/3542-bogot%C3%A1-es-una-ciudad-para-el-teletrabajo-c.html

Castro G. Mauricio. Surlatina Consultores. El nuevo estándar ISO para la Gestión del Riesgo en Chile. Disponible en: http://www.surlatina.cl/contenidos/archivos_articulos/13-el%20nuevo%20estandar%20iso%20para%20la%20gestion%20del%20riesgo.pdf

Cengage Learning. Introduction to Information Security [En línea]. http://www.cengage.com/resource_uploads/downloads/1111138214_259146.pdf

CEPAL. Lista de indicadores para el eLAC2015. Disponible en: http://archivo.cepal.org/pdfs/2013/S2013089.pdf

Colombia Digital. Una nueva firma del pacto por el teletrabajo. Disponible: http://colombiadigital.net/actualidad/noticias/item/7434-una-nueva-firma-del-pacto-por-el-teletrabajo.html

Colombia Digital. Teletrabajo en Iberoamérica Referentes y recomendaciones. Volumen 1. Bogotá D.C. Colombia, Agosto de 2013. Disponible en: http://colombiadigital.net/documentos/nuestras-publicaciones/item/5408-teletrabajo-en-iberoamerica-referentes-y-recomendaciones/5408-teletrabajo-en-iberoamerica-referentes-y-recomendaciones.html

CONGRESO DE LA REPÚBLICA. Ley 1221 de 2008. "Por lo cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones". 16 de julio de 2008. Disponible: http://www.mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-571.html

Corporación Colombia Digital. Memorias: Una nueva firma del Pacto por el Teletrabajo. Colombia, 25 de julio 2014. Disponible en: http://colombiadigital.net/actualidad/noticias/item/7434-una-nueva-firma-del-pacto-por-el-teletrabajo.html

Corporación Colombia Digital. Ministerio de las Tecnologías de la Información y las Comunicaciones. Libro Blanco el ABC del teletrabajo en Colombia. Bogotá D.C., Colombia Digital. 2012. Versión1.0.

Cyclopaedia. Economía y movilidad. Disponible en: http://www.puromarketing.com/12/18481/economia-movilidad-convierten-cafeterias-espacios-oficina-virtuales.html

Decreto reglamentario. Ley 1221 de 2008 teletrabajo. Colombia, 2008. Disponible: http://mintrabajo.gov.co/component/.../doc.../1876-ley1221de2008.html
Decreto 884 de 2012. Ministerio de trabajo. Disponible: http://www.mintic.gov.co/portal/604/articles-3638_documento.pdf

Decreto 1377 Consulta de la norma. Disponible: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

El mundo. Ventajas y desventajas del teletrabajo. Disponible en: http://www.elmundo.es/economia/2015/04/23/5537a77b22601dc5728b4581.html

EUROFOUND. Teletrabajo en la Unión Europa. En: http://www.eurofound.europa.eu/pubdocs/2009/961/es/1/EF09961ES.pdf

LIBRO BLANCO DEL ABC DEL TELETRABAJO EN COLOMBIA VERSION 3.0 Ministerio de las Tecnologías de la Información y las Comunicaciones, Bogotá D.C

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: presentación de tesis, trabajos de grado, y otros trabajos de Investigación. 6 ed. Bogotá D.C: INCONTEC, 2008 (NTC 1486)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: referencias bibliográficas. Contenido, forma y estructura. 6 ed. Bogotá D.C: INCONTEC, 2008 (NTC 5613)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: referencias documentales para fuentes de información electrónicas. 6 ed. Bogotá D.C: INCONTEC, 2010 (NTC 4490)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Trabajos escritos: Gestión del riesgo. Principios y Directrices. 6 ed. Bogotá D.C: INCONTEC, 2011 (NTC-ISO 31000)

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN Trabajos escritos: presentaciones y referencias bibliográficas. NTC-ISO31000.Bogotá D.C. ICONTEC, 2011

Jeffrey L. Whitten, Lonnie D. Bentley, Kevin C. Dittman . Systems Analysis and Design Methods. McGraw-Hill Irwin, 2004

Mark Rhodes – Ousley , Information Security segunda edición, Mac Graw Hill 2013

Ministerio de Tecnologías de la Información y Comunicaciones. Teletrabajo. Disponible en: http://www.mintic.gov.co/portal/604/w3-propertyvalue-571.html

Ministerio de Tecnologías de la Información y Comunicaciones. Teletrabaje con Seguridad. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-5106.html

NIST SP 800-46 Guide to Enterprise Telework and Remote access security

Purificación Aguilera. Seguridad Informática, 2010 Editex

Rodríguez Roger. Mejoramiento de las buenas prácticas de seguridad informática en el teletrabajo a través de una herramienta web. Tesis de grado. Universidad Piloto de Colombia. Facultad de Postgrados. Colombia, 2013.

UNIVERSIDAD DEL CAUCA. Conceptos Básicos de Sistemas de Información Disponible en: http://fccea.unicauca.edu.co/old/siconceptosbasicos.htm [citado en 5 noviembre de 2014]